

Universitat de Lleida

Escola Politècnica Superior

Enginyeria Tècnica en Informàtica de Gestió

Treball de final de carrera

**Creació d'un entorn Servidor d'accés wi-fi, usuaris i configuracions,
fent servir un Live CD.**

Autor: Josep Maria Ribes Companys

Directors: Fernando Guirado Fernández i Albert Cos Sánchez

Setembre 2008

Agraïments

Als companys que he conegut i que m'han ajudat
d'alguna forma durant aquests anys d'estudis

Als directors del projecte, en Fernando i l'Albert,
que sempre m'han guiat i ajudat durant l'elaboració
d'aquest treball

Al centre IES Torre Vicens, que m'ha donat la
possibilitat de realitzar aquest treball i en especial
a l'Albert, el Sisco i l'Eduard

A la meva família per donar-me la
possibilitat d'estudiar i recolzar-me SEMPRE

A la meva novia Isabel, per la enorme paciència,
comprensió, suport i ànims que m'ha brindat durant
aquests anys d'estudi

I sobretot al meu pare, que
sempre ha estat en mi i m'ha ajudat
a arribar al final d'aquests estudis

Resum

Amb aquest treball de fi de carrera es pretén posar en funcionament un servidor de dades d'usuaris, configuracions i accés a la xarxa sense fils fent servir un Live CD.

Es tracta d'ampliar els serveis que vol oferir un Institut de Secundaria, ja que en els últims temps ha sorgit la demanda de disposar de certes funcionalitats i facilitats que ajudarien a millorar l'entorn de treball del centre educatiu.

Entre aquestes millores hi figuren:

- La creació d'un espai privat de treball per a cada usuari.
- La gestió automatitzada dels usuaris del centre.
- La implantació d'una xarxa sense fils controlada per un portal captiu.

Per l'elaboració del projecte s'ha tingut en compte:

- La disponibilitat del sistema.
- El cost en diners de la implantació.
- La complexitat de la implantació del sistema.
- La possibilitat d'ampliació del nombre de serveis.

Per complir tots aquest principis s'ha decidit utilitzar Programari Lliure, ja que ens aporta:

- Un cost 0 en quant a llicències d'utilització.
- Ens proporciona possibilitat d'expansió del sistema.
- Ens garanteix estabilitat, disponibilitat i molt suport, tant a través de bibliografia, com en pàgines web oficials dels propis serveis.

Índex

Capítol 1: Raó de ser.....	9
1. Introducció.....	9
2. Objectius.....	10
Capítol 2: Anàlisi de requeriments.....	12
1. Problemàtica inicial.....	12
2. Tecnologies utilitzades.....	12
2.1. Software utilitzat.....	13
2.2. Hardware utilitzat.....	15
Capítol 3 : Solució proposada	17
1. Comparativa entre servidors Windows Server i Linux.....	17
Capítol 4 : Instal·lació del Servidor PDC.....	22
1. Guia d'instal·lació del servidor.....	22
2. Serveis necessaris per a la posada en funcionament del PDC.....	34
3. Instal·lació i configuració del sistema de quotes de disc.....	38
4. Instal·lació dels serveis per al procés de validació dels usuaris wi-fi.....	40
5. Extracció dels fitxers de configuració.....	44
6. Backup del PDC.....	46
7. Instal·lació i administració del servidor amb Webmin.....	51
Capítol 5: Instal·lació del Portal captiu.....	54
1. Instal·lació de Pfsense.....	54
2. Configuració del Portal captiu per fer les validacions d'usuaris al PDC.....	72
3. Punts d'accés sense fils.....	78
Capítol 6: Creació del Live CD.....	82
1. Guia de creació del Live CD.....	82
2. Opcions en la creació d'un Live CD.....	83
3. Instal·lació del Live CD.....	85

4.	Importació de la configuració del PDC.....	86
Capítol 7: Inserció dades d'usuari al sistema.		89
1.	Exportació de dades de SAGA.....	89
2.	Inserció de dades a la IntraWeb i Moodle.	89
3.	Importació de dades al Servidor PDC.....	100
4.	Automatització de creació del directori d'usuaris.	101
5.	Menú d'administració del sistema.....	103
Capítol 8: Conclusions.....		105
Capítol 9: Treballs futurs.		108
Annex.		109
	Llicència GPL.....	109
	Canvi de contrasenya en els diferents serveis.	121
Webgrafia		123
Glossari		125

Índex de figures

Figura 1: Exemple de dispositiu Embedded	14
Figura 2: Característiques Windows.....	18
Figura 3: Característiques Linux	18
Figura 4: Creació contenidors al PhpLDAPAdmin.....	26
Figura 5: Taula de grups d'usuaris del servei Samba.	27
Figura 6: Creació dels grups d'usuaris.	28
Figura 7: Alta d'usuaris de forma manual.	31
Figura 8: Configuració dels atributs del PDC.	33
Figura 9: Contingut del fitxer fstab.	39
Figura 10: Resultat de la comanda "mount".	40
Figura 11: Exportació de fitxers des de WinSCP i Windows.	45
Figura 12: Exportació de fitxers des de Konqueror i Kubuntu.	46
Figura 13: Reconeixement dels disc extern.	48
Figura 14: Edició del fitxer /etc/fstab	49
Figura 15: Muntat del disc extern.	49
Figura 16: Configuració de rsync amb cron i Webmin.....	51
Figura 17: Pantalla principal de Webmin.....	53
Figura 18: Pantalla de benvinguda de l'instal·lador de FreeBSD.	54
Figura 19: Creació de VLAN.	55
Figura 20: Configuració de les interfícies de xarxa (LAN).	56
Figura 21: Configuració de les interfícies de xarxa (WAN).....	56
Figura 22: Confirmació de la configuració escollida.	57
Figura 23: Instal·lar el sistema al Disc dur de l'ordinador.	57
Figura 24: Confirmació de la configuració de l'entorn triada.	58
Figura 25: Començament del procés d'instal·lació.	59
Figura 26: Selecció del disc on s'instal·larà el sistema.....	59
Figura 27: Formatació del disc.	60
Figura 28: Confirmació dels paràmetres del disc.	60
Figura 29: Confirmar la ordre de formatejar.	61
Figura 30: Particionament del disc.	61
Figura 31: Confirmació de les opcions de particionament.....	62

Figura 32: Confirmació del particionament.....	62
Figura 33: Formatació realitzada amb èxit.	63
Figura 34: Selecció de la partició formatada.	63
Figura 35: Avís de que es perdràn les dades existents del disc.....	64
Figura 36: Partició formatada amb èxit.....	64
Figura 37: Confirmar les opcions de creació de les particions.	65
Figura 38: Elecció del kernel que s'instal·larà.	65
Figura 39: Instal·lació dels bootblocks.....	66
Figura 40: Èxit en la instal·lació dels Bootblocks.....	66
Figura 41: Reiniciar el sistema.	67
Figura 42: Configuració de les interfícies de xarxa.	68
Figura 43: Establiment del rang de direccions del servidor DHCP.....	69
Figura 44: Confirmació de les opcions escollides.	69
Figura 45: Pantalla inicial del Pfsense.....	70
Figura 46: Configuració inicial del Pfsense.	71
Figura 47: Establiment de la configuració de les interfícies de xarxa.....	72
Figura 48: Configuració del Portal Captiu.....	73
Figura 49: Configuració de l'apartat RADIUS del Pfsense.	74
Figura 50: Configuració del Servidor HTTPS.	75
Figura 51: Esquema de funcionament del protocol HTTPS.	75
Figura 52: Configuració del Pass-through.....	76
Figura 53: Pantalla de Back Up del Pfsense.....	77
Figura 54: Detecció de les xarxes sense fils.	79
Figura 55: Pàgina web de benvinguda del Portal Captiu.....	80
Figura 56: Pàgina d'error d'autenticació.....	80
Figura 57: Pàgina web on serem redireccionats i finestra emergent de desconnexió.....	81
Figura 58: Accés al mòdul d'administració de la Intraweb.....	90
Figura 59: Pàgina de gestió d'usuaris de la Intraweb.....	91
Figura 60: Format de la taula d'usuaris de la Intraweb.....	91
Figura 61: Aclaració sobre els grups d'usuaris de la Intraweb.	92
Figura 62: Inici del procés d'importació.	93
Figura 63: Primer pas d'importació realitzat correctament.	93
Figura 64: Gestió dels usuaris importats.	94

Figura 65: Confirmació de les dades de connexió dels usuaris.	95
Figura 66: Repàs de les ordres donades.	95
Figura 67: Confirmació de la inserció dels usuaris a la Intra web.	96
Figura 68: Pàgina d'importació de dades al Servei LDAP.....	101
Figura 69: Canvis de contrasenya.....	122

Capítol 1: Raó de ser.

1. Introducció.

Aquest treball de fi de carrera està enfocat a la implantació d'una estructura client servidor en un centre d'Educació Secundària, concretament a l'IES Torre Vicens de Lleida. Per tant, totes les decisions preses sobre el funcionament i aplicació del projecte han estat consensuades entre l'alumne que ha realitzat el treball i el coordinador d'informàtica del centre en qüestió.

Per altra banda, aquest treball podrà servir com a guia per la implantació d'aquest sistema en qualsevol institució que necessiti una estructura de funcionament similar, com per exemple algun altre institut de secundària.

Aquest projecte pretén donar suport en la gestió de les dades dels professors, alumnes i personal d'administració i serveis del centre. A més, també permetrà ampliar el nombre de serveis que el centre pot oferir, ja que amb aquest projecte es durà a terme una reestructuració de l'àmbit informàtic al centre.

En l'actualitat el centre disposa de 180 ordinadors repartits en 5 aules d'informàtica, departaments i aules equipades amb projectors. Amb aquest projecte es pretén fer que tots aquest ordinadors depenguin de les dades i configuracions emmagatzemades en un Servidor que es vol implantar. A més, el centre també disposa de cobertura wi-fi per tal de donar servei al personal que ve al centre amb els seus propis dispositius i també a departaments, on fer-hi arribar un punt de connexió de xarxa resulta inviable degut a l'alt cost que tindria en comparació a la instal·lació d'un dispositiu inal·làmbic standard. El centre ja disposa d'un servidor de dades propi on s'emmagatzemen totes les dades del personal del centre. Aquest, però té una sèrie de limitacions o inconvenients que el fan poc òptim a l'hora de preservar la confidencialitat de la informació que hi ha disponible, ja que els usuaris no tenen un espai privat on emmagatzemar les seves dades.

En aquest treball de fi de carrera també es pretén crear un Live CD [27] que ens ajudi a posar en funcionament un servidor capaç de contenir, validar i controlar les dades dels usuaris que estan dins de la xarxa en qüestió.

La problemàtica que ha de resoldre aquest projecte es pot resumir amb els següents punts:

- Donar d'alta a totes les persones que formen el centre als serveis web que el mateix centre vol oferir. Aquest serveis són la IntraWeb i el Moodle, dues eines de comunicació i treball que el centre i el personal del centre utilitzen diàriament.
- Automatitzar en la mesura de lo possible la inserció de les dades dels alumnes als serveis avanç esmentats i aprofitar aquestes dades per augmentar les funcionalitats i serveis del centre.
- Unificar les dades de connexió del personal del centre per tal de facilitar la utilització d'aquests serveis i a més, a part de l'accés als serveis web des del centre, donar als usuaris un espai privat i personal de treball, i la possibilitat de connectar-se a Internet mitjançant la xarxa sense fils.

2. Objectius.

Per tal de facilitar la implantació d'aquest sistema es crearà una pròpia distribució de Linux en format Live CD. Aquesta distribució ja incorporà tots els serveis necessaris instal·lats. A més es disposarà del programari necessari per a reconvertir les dades del personal i importar-les directament al PDC. Aquest Live CD inclourà el programari necessari per a realització de les còpies de seguretat i restauració, i els fitxers de configuració dels serveis. Aquests fitxers de configuració estaran adaptats al cas real d'aplicació, però també es podran modificar per qualsevol usuari que vulgui implantar aquesta infraestructura.

En resum, els objectius són:

- Crear una guia d'instal·lació que permeti al personal inexpert del centre a entendre el funcionament dels serveis, ampliar els serveis si s'escau, resoldre les possibles fallides del sistema, i restablir els serveis.
- Implantació d'un PDC (Controlador de Domini Principal)
- Còpies de seguretat dels usuaris.
- Implantació d'un Portal Captiu [2] (Per controlar accessos dels usuaris wi-fi).

- Creació d'un Live CD amb tots els serveis instal·lats i configurats per facilitar la implantació del Sistema.
- Importació de les dades d'usuaris als serveis.
- Tractament de les dades de connexió d'usuaris per facilitar la importació massiva al PDC.

Capítol 2: Anàlisi de requeriments.

1. Problemàtica inicial.

Aquest projecte presenta la problemàtica inicial de donar d'alta a un gran nombre d'usuaris al sistema. Es tracta d'un centre educatiu molt gran si el comparem amb la resta d'Instituts de la província, ja que hi imparteixen estudis més de 1100 alumnes. A més també hi un grup molt nombrós de professors (110 aproximadament), i el personal del PAS (Personal Administració i Serveis). Per tant, el fet de donar d'alta al sistema a tots aquest usuaris seria un procés llarg i costós que cal automatitzar o realitzar de la forma més senzilla possible, per tal de que el personal que ha d'administrar el sistema tingui les màximes facilitats a l'hora de gestionar les dades del personal del centre.

A més de l'alta d'usuaris als nous serveis que es volen oferir, també cal facilitar la posada en funcionament d'aquest serveis. Per això, en aquest projecte també caldrà donar una explicació de com s'han de donar d'alta aquest serveis i quines tecnologies s'han utilitzat per implantar-los. Per facilitar encara més les tasques d'implantació del sistema es crearà un Live CD que ja portarà els serveis instal·lats.

Per tant, la problemàtica es podria resumir en l'alta del personal de forma massiva a tots els serveis que el centre vol oferir. Aquesta alta automatitzada ha de servir per a simplificar la gestió dels usuaris del centre. A més les dades de connexió dels usuaris a tots els serveis han de ser, almenys des d'un principi, les mateixes. D'aquesta forma els usuaris podran accedir a tots els serveis amb les mateixes dades de connexió, fet que es creu important ja que la majoria d'usuaris no vol recordar-se de tantes dades de connexió diferents. Els usuaris que vulguin canviar aquestes dades de connexió ho podran fer des dels mateixos serveis on estan donats d'alta.

2. Tecnologies utilitzades.

Per a la implantació del sistema hem optat per a la utilització de Programari Lliure i per aprofitar el maquinari del qual ja disposa el centre. Per tant, el

cost de la implantació del sistema només vindrà determinat pel temps que triguem en ficar el sistema en funcionament.

2.1. Software utilitzat.

2.1.1. Distribució Linux utilitzada per la creació del Live CD.

El sistema operatiu que permetrà ficar en funcionament tots els serveis, i que a la vegada ens permetrà crear el Live CD és la distribució de Linux Debian. Dins de les versions de Debian utilitzarem la versió “stable” (estable) ja que no ens podem permetre el luxe d'arriscar-nos a implantar programari que encara no està prou testat i que no ens aporta garanties d'estabilitat i correcte funcionament.

Al mercat ja existeixen diverses distribucions que ens ofereixen la possibilitat d'implantar un sistema d'aquestes característiques. En el nostre cas, però, hem optat per implantar els serveis disposant del sistema base (la distribució Debian) i exclusivament els paquets necessaris per a la implantació del sistema. Amb això garantim un òptim funcionament del sistema, ja que només hi tenim funcionant els serveis necessaris, i una personalització més acurada dels serveis. A més, el fet d'utilitzar aquesta distribució ens allibera d'utilitzar programari amb llicències més o menys cares o de treballar amb versions limitades d'aquestes distribucions ja comentades.

Algunes de les distribucions que ja tenen “preconfigurats” aquests serveis són:

- Clark Connect <http://www.clarkconnect.com>
- eBox <http://ebox-platform.com/>
- OpenFiler <http://www.openfiler.com/>

2.1.2. Distribució BSD per a la gestió del Portal Captiu (PfSense).

Per la gestió i configuració del Portal Captiu s'ha escollit una solució software com és la distribució PfSense basada en FreeBSD [3].

PfSense és gratuït, de codi lliure i es tracta d'una personalització de la distribució FreeBSD per utilitzar-lo com a router o tallafocs

(firewall). A més de ser molt potent, de ser flexible i d'oferir una plataforma d'enrutament molt robusta, aquest software inclou una immensa llista de funcionalitats relacionades i un sistema de paquets (els disponibles per BSD) que ens permeten ampliar el sistema fàcilment. Pfsense és un projecte popular amb més d'un milió de descarregues des de la seva creació, i que demostra diàriament la seva capacitat de protecció tant en instal·lacions domèstiques com en grans empreses, universitats o altres organitzacions.

PfSense també permet la possibilitat d'instal·lar el software en memòries compact flash per a dispositius Embedded. Un exemple de dispositiu Embedded:



Figura 1: Exemple de dispositiu Embedded

El FX5620 és un sistema de baix consum d'energia que treballa amb un processador VIA de 1 Ghz. El sistema no té ventilador i pot funcionar des d'una targeta Compact Flash o des d'un disc dur de 2,5" (els dels ordinadors portàtils). La memòria RAM està formada per un mòdul de RAM SoDIMM de 256 Mb.

Aquest dispositiu incorpora 6 targetes de xarxa, de les quals 5 treballen a 10/100 Mbits i l'altra a Gigabit. També disposa de connector de teclat i ratolí, sortida VGA per monitor, 2 connectors USB i un connector Serial RS-232. La placa base del mini-pc també disposa d'un slot on es pot connectar, per exemple, un dispositiu inal·làmbic.

2.1.3. Distribució per al dispositiu sense fils.

Per als dispositius que donen accés sense fils als usuaris utilitzarem el software que ja porta instal·lat el propi dispositiu i en alguns casos, modificarem aquest firmware per tal d'aconseguir

més funcionalitats. En el cas dels Linksys, utilitzarem el que ja porten instal·lat.

Per altra banda també disposem d'alguns dispositius molt econòmics adquirits a molt bon preu a través de la plataforma WI-FI FON [4]. Aquests dispositius porten un firmware modificat pel propi distribuïdor FON. El que hem fet nosaltres ha estat modificar aquest firmware implantant-ne un de millor i gratuït que ens ofereix més possibilitats de configuració. Es tracta del firmware provinent del projecte DD-WRT.

DD-WRT és un firmware lliure per a diversos routers inal·làmbrics, és molt comú trobar-lo en equips Linksys WRT54G. Executa un reduït sistema operatiu basat en Linux. Està sota la llicència GNU General Public License [5].

2.2. Hardware utilitzat.

2.2.1. Per al servidor PDC (Primary Domain Controller).

Per al Servidor PDC utilitzarem un Ordinador del Fabricant Dell. Es tracta d'un model de la família de Servidors d'aquesta companyia. L'elecció de implantar-ho en un Servidor com aquest és que aquest servidor ens proporciona certes garanties d'estabilitat i disponibilitat.

Les característiques del Servidor són:

- Processador Intel Xeon amb un processador a 2,8 Ghz.
- 2 GB de Memòria RAM.
- Controladora RAID amb un RAID 5 configurat. (3 Discs Durs de 160 GB).
- 2 Targes de Xarxa Gigabit

2.2.2. Per al Portal captiu.

Per al Portal captiu també utilitzarem un ordinador del fabricant DELL. Es tracta d'un ordinador de la gamma mitja d'aquest fabricant. El model exacte de l'ordinador és el GX 270. És un

ordinador prou potent i estable que ens ofereix altes garanties d'estabilitat i disponibilitat.

Les característiques d'aquest ordinador són:

- Processador Intel Pentium 4 a 2,8 Ghz
- 512 MB de memòria RAM.
- Disc Dur de 40 GB.
- Tarja de Xarxa Intel Gigabit (WAN).
- Tarja de xarxa 10 / 100 (LAN).

2.2.3. Dispositius Sense fils.

Un dels avantatges més importants que ens proporcionarà el fet de disposar d'un ordinador on hi tenim instal·lat el portal captiu, es que d'aquesta forma es centralitza el control de tots els dispositius ja que tots aquest utilitzen el portal captiu per a fer les validacions.

Comentem aquest fet perquè hi ha molts dispositius que ja porten implementada l'opció de realitzar les autenticacions contra un servidor RADIUS. En el nostre cas utilitzarem punts d'accés inal·làmbrics molt més econòmics i que no disposen d'aquesta funcionalitat. Per tant, utilitzant punts d'accés molt més econòmics i a més utilitzant programari lliure per al Portal Captiu reduïrem molt el cost de la implantació dels serveis.

El centre ja disposa d'alguns dispositius inal·làmbrics, majoritàriament del fabricant Linksys. Són dispositius de la gama baixa d'aquest fabricant i compleixen les funcionalitats bàsiques, que en el nostre cas, ja són més que suficients. A més dels Linksys també disposem de dispositius de la plataforma WI-FI FON, que un cop modificats amb el firmware DD-WRT els hi podem assignar les funcionalitats desitjades.

Aquest dispositius sense fils s'hauran de configurar en mode Punt d'accés (també es poden configurar en mode Bridge (Pont)) i els paràmetres de configuració de la xarxa hauran d'estar dins el mateix rang de xarxa del Portal captiu per tal de que els dispositius i el Portal Captiu es puguin comunicar.

Capítol 3 : Solució proposada

1. Comparativa entre servidors Windows Server i Linux.

En aquest projecte hem hagut d'escollir entre dos sistemes operatius, per una banda el Windows 2000 Server i per l'altra alguna distribució de Linux.

Actualment tots els centres de Secundària estan dotats amb un ordinador que actua com a servidor i que disposa d'una llicència de Windows 2000 Server. Aquest servidor ja està "preconfigurat" pel Departament d'Educació i a més aquest mateix facilita una "maqueta" per restaurar el Servidor en cas de fallida. En el cas del centre on he d'implantar el Servidor PDC ja fa temps que s'ha prescindit d'aquest ordinador ja que mai ens ha aportat una certa estabilitat i protecció de dades.

A l'hora de tirar endavant el projecte es va proposar la solució de ficar en funcionament els serveis que es volien implantar en aquest servidor Windows però no es va trigar gaire a desestimar aquesta opció per diversos motius. Aquests motius venien impulsats per la dependència d'un sistema desconegut pel personal del centre i també pels tècnics que el Departament d'educació envia als centres en cas d'averies. Aquest fet provocava que el centre havia de buscar recolzament extern al centre i a un cost força elevat.

A més, durant aquests últims anys, des del propi centre i des del Departament d'ensenyament s'està impulsant la utilització de programari lliure ja que ens deslliga de llicències d'utilització i ens ofereix els avantatges del baix cost i de l'estabilitat del sistema.

Amb aquests motius ja en hi ha prou per creure fermament en la utilització del programari lliure per a la implantació del Servidor.

A més d'aquests raonaments, també hi ha avantatges i inconvenients de tots dos sistemes que ens fan decidir per un o altre sistema. següents:

Avantatges i Inconvenients de Windows Server

Avantatges	Inconvenients
Fàcil d'utilitzar, interfície familiar.	Llicència cara.

Tots els altres ordinadors amb Windows es connecten de forma nativa.	Risc d'infecció per virus i vulnerabilitats del sistema.
Suport per molts fabricants.	Part dels software és car.
	Alts requisits de maquinari.

Figura 2: Característiques Windows

Avantatges i Inconvenients de Linux

Avantatges	Inconvenients
La majoria de les distribucions són gratuïtes.	Dificultat d'aprenentatge.
Generalment és més segur i estable.	Falta de títols populars de programari.
Suport per molts fabricants.	La personalització del Sistema operatiu pot ser complexa.
No està afectat per virus.	
No requereix un maquinari molt potent.	
Pot conviure amb Windows.	

Figura 3: Característiques Linux

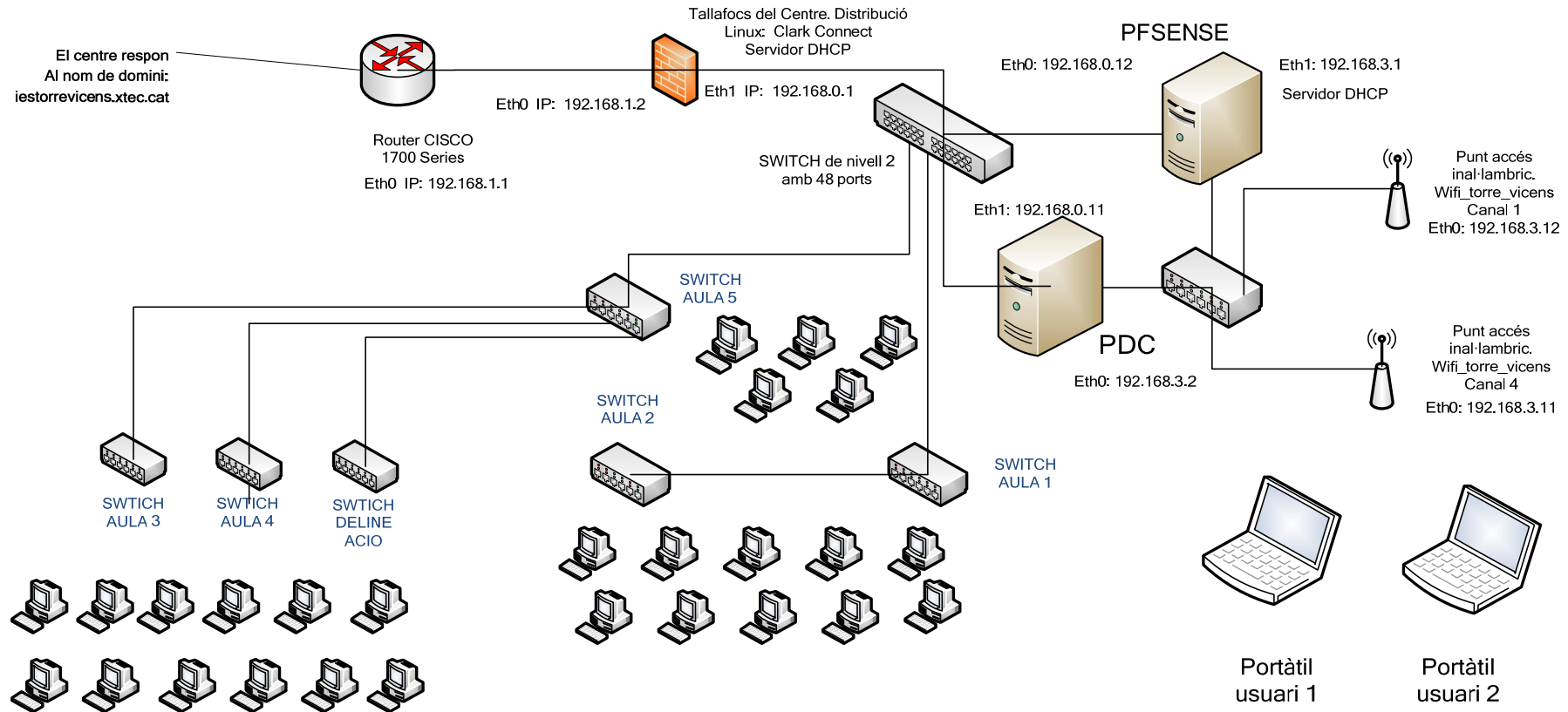
Un cop vistos els avantatges i inconvenients de tots dos sistemes anem a exposar el que necessita el centre:

- Baix cost de llicències.
- Baix requeriment de maquinari.
- Estabilitat i disponibilitat del sistema.
- Molta documentació per a poder solucionar els problemes i/o ampliar els serveis del Servidor.
- Escalabilitat. Ampliar els serveis del servidor fàcilment.

Un cop vistes les necessitats del centre veiem que el sistema operatiu més assequible per al Servidor és Linux, ja que aquest compleix tots els requeriments avanç esmentats.

En les següent figures, esquema físic (Figura 4) i esquema lògic (Figura 5), es pot observar quina solució s'aplica per a implantar tot el sistema.

ESQUEMA FÍSIC



Els  estàn dins del domini INTRACENTRE creat al PDC.

Tots els equips tenen adreces de la xarxa cablejada 192.168.0.0.

Portàtil usuari 1 Portàtil usuari 2

Es connecten de forma inal·làmbrica als punts d'accés del portal captiu.

Aquests usuaris No estan donats d'alta al DOMINI INTRACENTRE

Aquest dispositius portatils estan conetats a la xarxa inal·làmbrica 192.168.3.0 creada pel PFSENSE.

Figura 4: Esquema Físic

ESQUEMA LÒGIC

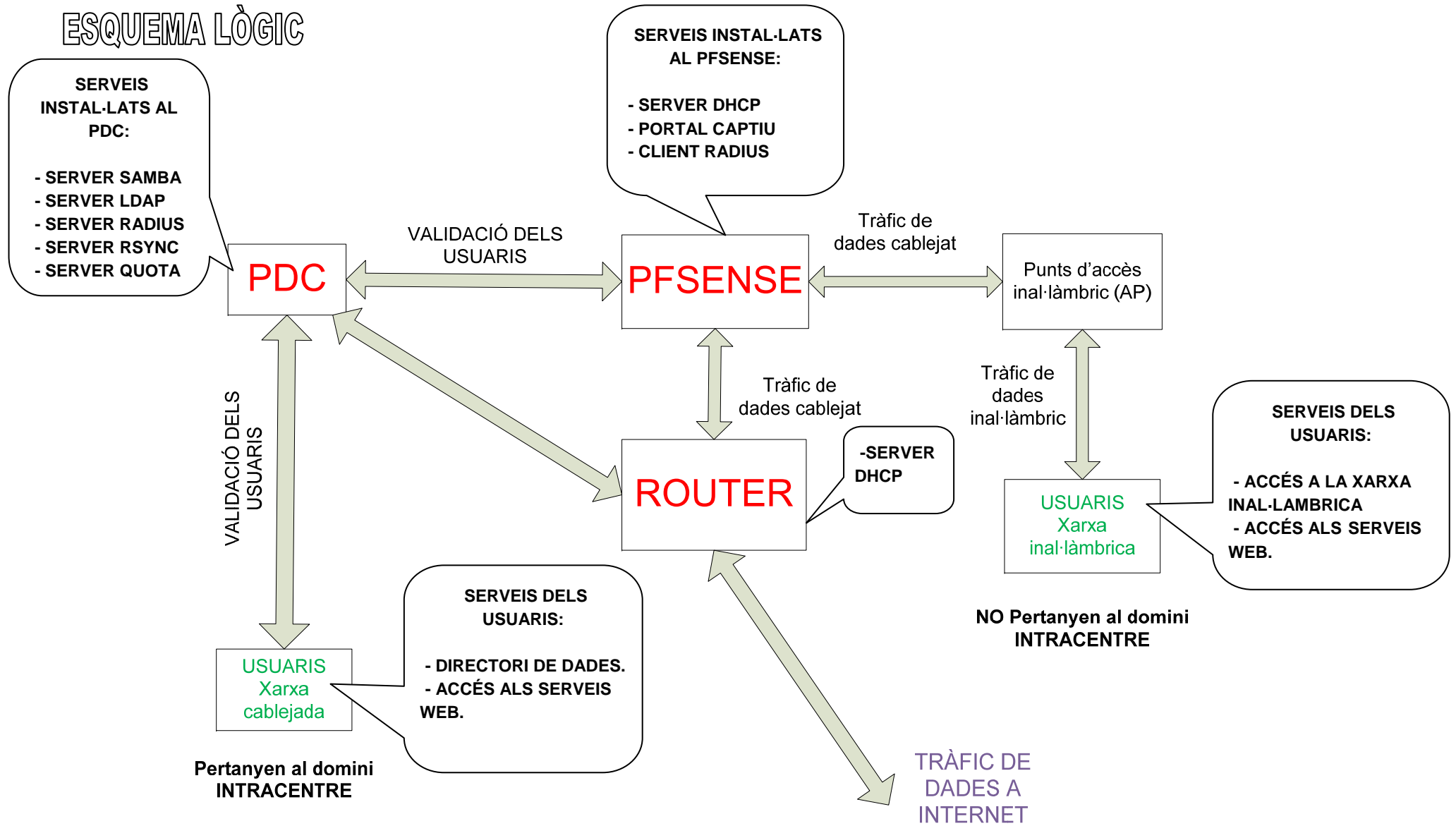


Figura 5: Esquema Lògic

Capítol 4 : Instal·lació del Servidor PDC

1. Guia d'instal·lació del servidor.

Per a poder crear un Live CD que ens faciliti les tasques d'instal·lació i administració d'un Controlador de Domini Principal (PDC) primerament cal conèixer com funcionen i com es fiquen en funcionament tots aquest serveis.

Per tant, el primer que anem a fer es donar una guia de com instal·lar tots els serveis. En el proper apartat explicarem que és i per a que serveix cada servei. D'aquesta forma obtindrem les bases per a després, administrar i controlar com cal un Servidor d'aquestes característiques.

Tal i com hem esmentat en l'anterior capítol, la distribució de Linux triada per a ficar en funcionament el PDC és Debian, amb la seva versió estable (Etch). Nosaltres hem triat la distribució que a més del paquets bàsics disposa d'un entorn gràfic, en aquest cas lleuger (XFCE) [6], per a que l'usuari no tant expert pugui moure's pel servidor i gestionar-lo mitjançant un entorn gràfic. També podríem utilitzar la versió estable que no disposa d'entorn gràfic i que s'instal·la des dels repositoris de Debian (Netinstall). D'aquesta forma ens estalviaríem el fet de instal·lar programes innecessaris i el tamany del Live CD es reduiria de forma considerable.

Primerament fem una instal·lació del Sistema Operatiu Debian sobre l'ordinador que hem escollit com a servidor. Seguirem els passos d'instal·lació que ens marca l'assistent i els haurem d'adaptar a les nostres necessitats. Una d'elles és escollir la configuració de les interfícies de xarxa. En aquest cas indicarem la configuració de forma manual, ja que volem tenir documentada tota la informació referent a la configuració del servidor. I en segon lloc li direm que ens munti la partició `/home` separada en una altra partició, ja que volem tenir les dades separades de la configuració del servidor. Un cop triades aquestes característiques i el sistema instal·lat, només ens caldrà iniciar el servidor i validar-nos amb les dades d'usuari que hem facilitat en el procés d'instal·lació per a poder accedir a administrar el sistema. Un cop dins el sistema obrim el "terminal" i comencem la instal·lació manual del nostre PDC:

Per a fer qualsevol canvi en un sistema Linux basat en Debian cal que davant de cada instrucció introduïm la instrucció: `"sudo"` seguit del

password del administrador del sistema. Amb això li direm al sistema que som els administradors i que tenim l'opció de modificar les configuracions del Servidor.

Llegenda del següent apartat:

- Instruccions de línia de comandes.
- Comentaris aclaratoris sobre el que s'està fent.
- Informacions que ens demana la pròpia instal·lació del servidor.
- *Contingut dels fitxers de configuració dels serveis instal·lats.*

Habilitem l'accés al Servidor mitjançant connexions SSH

```
#apt-get install openssh-server
```

Reiniciem el servei per comprovar que l'hem instal·lat correctament i ja podrem accedir al sistema mitjançant la direcció IP del servidor des de qualsevol ordinador.

```
#!/etc/init.d/ssh restart
```

Primerament actualitzarem el sistema:

```
#apt-get update  
#apt-get upgrade
```

Instal·lem les dependències necessàries:

```
#apt-get install make gcc gcc++ gengetopt libpopt-dev  
python-crypto
```

Instal·lació del servei LDAP

Ens demanarà que introduïm el password de l'administrador del servei LDAP.

```
#apt-get install slapd ldap-utils
```

Reconfigurem el servei LDAP contestant a les preguntes que se'ns formulin:

```
#dpkg-reconfigure slapd
```

A les preguntes contestem el següent:

Desea omitir la configuracion de ldap : no
Introduzca el nombre de dominio DNS : intracentre
Introduzca el nombre de su organizacion : intracentre
Contraseña del administrador : password
Verificación de la contraseña : password
Motor de base de datos a utilizar : BDB
Desea que se borre la base de datos cuando purge el paquete slapd :NO
Desea mover la base de datos antigua : SI
Permitir el protocolo LDAPV2 : si

Podem comprovar la correcta instal·lació del servei LDAP mitjançant:

```
#ldapsearch -x -b "dc=intracentre"
```

Instal·lació del Servidor web Apache-ssl. Contestem a les preguntes per a generar el certificat.

```
#apt-get install apache-ssl
```

Instal·lació de smbldap-tools

```
#apt-get install smbldap-tools
```

Instal·lació de phpldapadmin

```
#apt-get install phpldapadmin
```

Instal·lació de MKNTPWD. Aquest no es troba dins del paquet de programes de smbldap-tools, per tant, haurem de descarregar els fitxers font i compilar-los

```
#wget http://www.silcom.com.pe/soft/mkntpwd.tar.gz
```

```
#tar -zxvf mkntpwd.tar.gz
```

```
#cd mkntpwd
```

```
#make
```

```
#cp mkntpwd /usr/local/bin
```

Comprovem la correcta instal·lació executant el servei:

```
#mkntpwd
```

Instal·lació de Samba

A les preguntes contestem el següent:

Nombre del dominio o grupo trabajo: intracentre
Modificar smb.conf... : no

```
#apt-get install samba samba-doc
```

Creem carpetes per allotjar les configuracions de servei Samba

```
#mkdir /home/samba  
#mkdir /home/samba/netlogon  
#mkdir /home/samba/profiles
```

Configuració del Servei LDAP

```
#cd /usr/share/doc/samba-doc/examples/LDAP  
#gunzip samba.schema.gz  
#cp samba.schema /etc/ldap/schema  
#vim /etc/ldap/slapd.conf
```

Editem el fitxer slapd.conf i afegim la següent línia a continuació dels altres include

```
include /etc/ldap/schema/samba.schema
```

Reiniciem el servidor LDAP

```
#/etc/init.d/slapd restart
```

En aquest punt ja haurem inclòs al nostre arbre LDAP el domini: intracentre. Ara li donem forma a l'arbre creant els contenidors base */
Accedim a la web d'administració del Servei LDAP mitjançant el navegador web a la direcció: https://IP_Servidor/phpldapadmin/ i ens validem amb les dades de connexió introduïdes durant la instal·lació.

Login DN: cn=admin,dc=intracentre

Password: password

Un cop validats creem els contenidors base fent: "Create new entry here" i seleccionant l'opció: "Organisational Unit" seguit de "Proced", i introduïm "users". Repetim el mateix dos cops més amb la creació de "machines" i "groups".

L'arbre ha de quedar així:

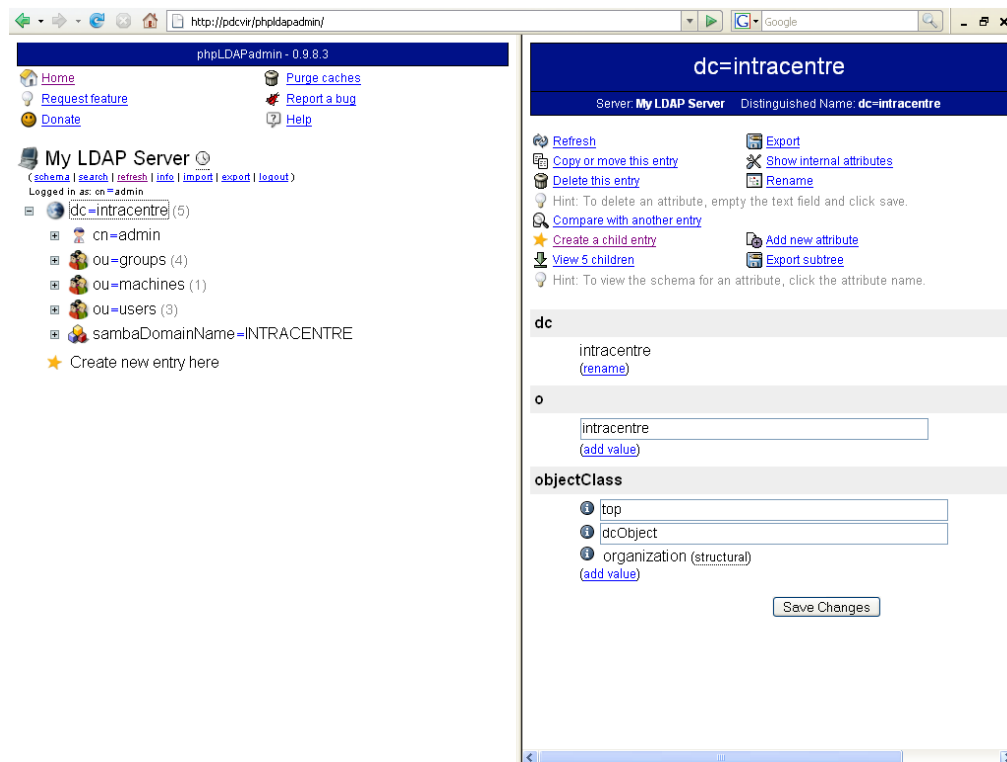


Figura 4: Creació contenidors al PhpLDAPAdmin.

Configuració del servei Samba i Backup de la configuració samba original.

```
#cd /etc/samba  
#cp smb.conf smb.conf.bkp
```

Editem el fitxer en funció de la configuració desitjada. Podrem establir: el nom del servidor, nom del grup de treball, el rang de xarxa on haurà d'escoltar les peticions dels usuaris, adaptació a l'estructura de l'arbre LDAP i directoris i recursos dels usuaris. Un cop establertes les configuracions, podem provar si la configuració es correcta mitjançant la instrucció:

```
#testparm
```

Li donem la contrasenya del Servei LDAP al Servei Samba per a que puguin interactuar tots dos serveis.

```
#smbpasswd -w password
```

Reiniciem el Servei Samba (`#/etc/init.d/samba restart`) i comprovem que s'ha creat l'entrada: "sambaDomainName=INTRACENTRE" dins el nostre arbre LDAP.

Creem els grups de domini entrant al contenidor "groups" i escollint la opció "New Samba3 Group Mapping". Haurem d'introduir la següent informació:

Nom Windows	Nom Unix	GID	RID	Comentaris sobre els grups
Domain Admins	sambaadmins	20000	512	Aquest grup d'usuaris tindran privilegis d'administració localment en els seus ordinadors. Per tant, podran instal·lar programes i fer les modificacions pertinents sobre els ordinadors.
Domain Users	sambausers	20001	513	Grup d'usuaris limitat localment. Només podran modificar les dades dels seus directoris personals.
Domain Guests	sambaguests	20002	514	Grup d'usuaris invitats. S'utilitzarà per donar accés a personal extern al centre.
Domain Computers	sambamachines	20003	515	Aquí es donaran d'alta els ordinadors que pertanyin al domini creat.

Figura 5: Taula de grups d'usuaris del servei Samba.

L'arbre del Servei LDAP quedarà així:

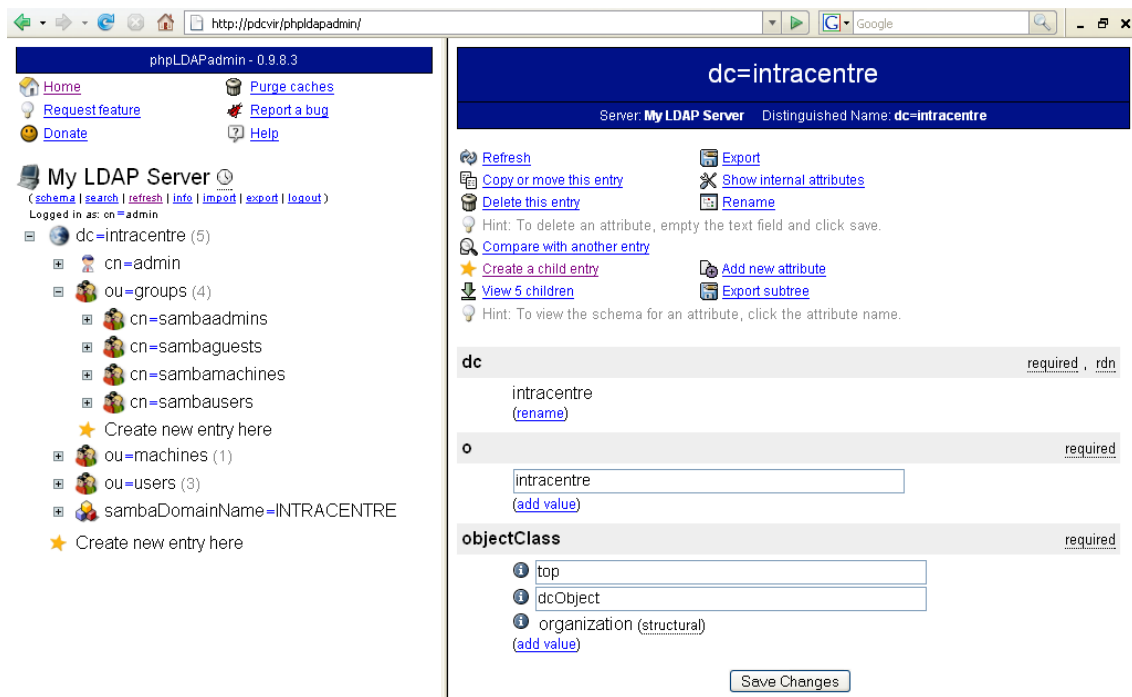


Figura 6: Creació dels grups d'usuaris.

Integració de l'autenticació i LDAP
Instal·lació NSS LDAP

#apt-get install libnss-ldap

Configuració del servei

#dpkg-reconfigure libnss-ldap

Servidor LDAP : 127.0.0.1

Nombre distintiu (DN) : dc=intracentre

Versió de LDAP a utilitzar : 3

Hace falta un usuario para acceder a la base de datos ldap : No

Dar privilegios especiales de ldap para root : SI

Desea hacer que la configuracion solo pueda leer o escribir el propietario : SI

Cuenta ldap para root : cn=admin,dc=intracentre

contraseña ldap para root : password

Per la configuració del servei cal editar el fitxer nsswitch.conf

#vim /etc/nsswitch.conf

Hem de comentar aquestes línies:

```
passwd: compat  
group: compat  
shadow: compat
```

I afegir aquestes:

```
passwd: compat ldap  
group: compat ldap  
shadow: compat ldap
```

Per comprovar que tot es correcte fem:

```
#getent group
```

Ens han d'aparèixer els grups creats juntament amb el seu GID.

Instal·lació PAM LDAP

```
#apt-get install libpam-ldap
```

Configuració del servei

```
#dpkg-reconfigure libpam-ldap
```

Servidor ldap : 127.0.0.1

Nombre distintivo : dc=intracentre

Vercion de ldap : 3

Make local root Database admin : si

Hace falta un usuario para la base de datos LDAP : no

Ldap account for root : cn=admin,dc=intracentre

contraseña para la cuenta ldap de root : password

Local crypt to use when changing passwords : md5

```
#vim /etc/pam.d/common-account
```

Comentar

```
account required pam_unix.so
```

I afegir

```
account sufficient pam_ldap.so  
account required pam_unix.so try_first_pass
```

```
#vim /etc/pam.d/common-auth
```

Comentar

```
auth required pam_unix.so nullok_secure
```

I afegir

```
auth sufficient pam_ldap.so  
auth required pam_unix.so nullok_secure  
use_first_pass
```

```
#vi m /etc/pam.d/common-password
```

Comentar

```
password required pam_unix.so nullok obscure min=4  
max=8 md5-
```

I afegir al final

```
password sufficient pam_ldap.so  
password required pam_unix.so nullok obscure min=4  
max=8 md5 use_first_pass
```

Instal·lació del servei NSCD

```
#apt-get install nscd
```

Reiniciar el Servei Samba

```
#/etc/init.d/samba restart
```

Agreguem els administradors i usuaris de prova al domini.
Anem al contenidor “users” i creem els següents usuaris amb les
següents dades: (Seleccionem l’opció “Create new entry” i després
“Samba3 Account”).

Fist Name : Administrator
Last Name : de la xarxa
Comon Name : administrator
User ID : administrator
UID Number : 0
Samba SID : 512
Password : password
Verify Password : password
Home Directory : /home/administrator

Fist Name : coordinador
Last Name : informatica
Comon Name : coordinador

User ID : coordinador
UID Number : 10000
Samba SID : 512
Password : password
Verify Password : password
Home Directory : /home/coordinador

Fist Name : usuari
Last Name : de prova
Comon Name : usuari
User ID : usuari
UID Number : 10001
Samba SID : 513
Password : passwordusuari
Verify Password : passwordusuari
Gid number : sambausers
Primary Group ID : sambausers
Home Directory : /home/usuari

L'arbre del Servei LDAP quedarà així.

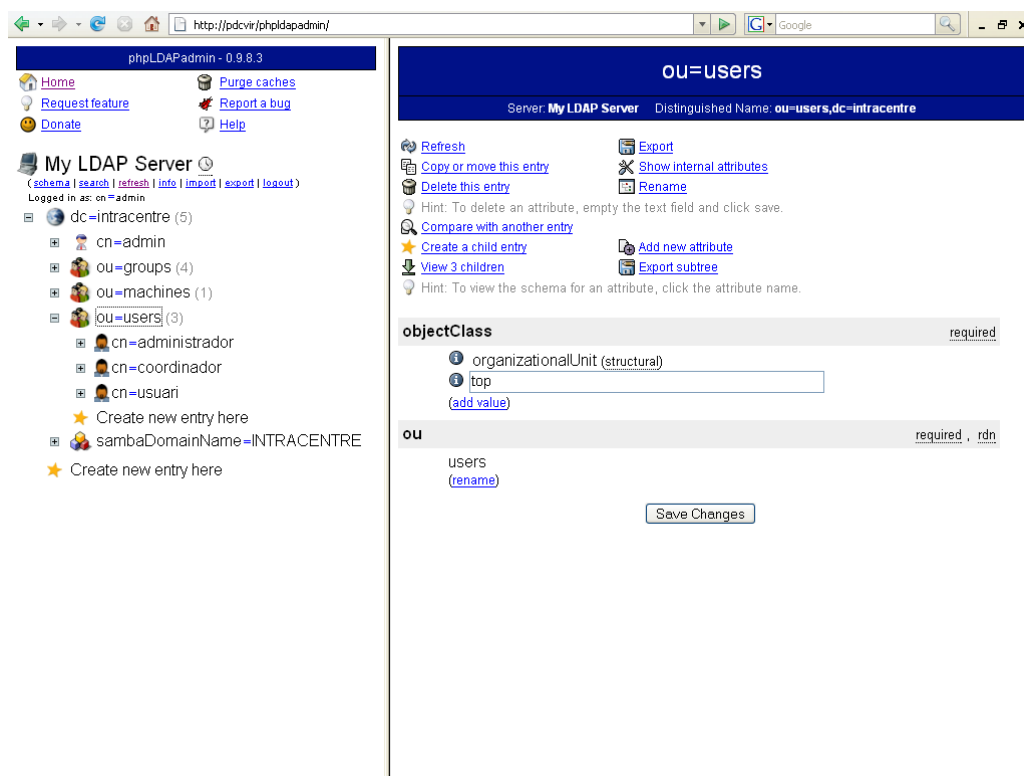


Figura 7: Alta d'usuaris de forma manual.

Comprovem que tot ha funcionat correctament

#getent passwd

Ens ha d'aparèixer:

```
admi ni strador: *: 20000: admi ni strador: /home/admi ni strad
or:
coordi nador: *: 10000: 20000: coordi nador: /home/coordi nad
or:
usuari : *: 10001: 20001: usuari : /home/usuari :
```

Creació dels home d'usuari (directoris dels usuaris)

Usuari administrador

```
#mkdi r /home/coordi nador
#cp /etc/skel /. * /home/coordi nador/
#chown -R coordi nador /home/coordi nador
#chgrp -R sambaadmi ns /hom/coordi nador
```

Usuari de proves

```
#mkdi r /home/usuari
#cp /etc/skel /. * /home/usuari /
#chown -R usuari /home/usuari
#chgrp -R sambausers /home/usuari
```

Automatització d'ingrés dels ordinadors a l'arbre LDAP

```
#cd /usr/share/doc/smbldap-tool s/exampl es
#cp smbldap. conf. gz smbldap_bi nd. conf /etc/smbldap-
tool s
#cd /etc/smbldap-tool s
#gunzi p smbldap. conf. gz
#chown root: root *
#chmod 600 *
```

Cal editar dos fitxers per completar l'automatització.

```
#vi m /etc/smbldap-tool s/smbldap_bi nd. conf
```

```
slaveDN="cn=admi n, dc=i ntracentre"
slavePw="password"
masterDN="cn=admi n, dc=i ntracentre"
masterPw="password"
```

Cal comprovar la configuració desitjada en el següent fitxer:

```
#vi m /etc/smbldap-tool s/smbldap. conf
```


Finalment, cal copiar els dos fitxers anteriors al directori /etc/

```
#cp smbldap_binds.conf /etc/
#cp smbldap.conf /etc/
```

Agreguem l'atribut: "SambaUnixIdPool":

Anem al phpldapadmin i fem clic sobre:

"SambaDomainName=INTRACENTRE", ara mirem a la dreta i busquem l'espai reservat per als atributs i seleccionem: "add value". Escollim l'opció "SambaUnixIdPool" i "Add new ObjectClass". Afegim els valor UID i GID amb els que ficarem en funcionament el nostre servidor. Per uidNumber introduïm 30000, nombre inicial amb que començarem a identificar els ordinadors del nostre domini. Per gidNumber escollim el 20003, ja que és el valor que hem assignat al grup sambamachines en els apartats anteriors.

L'arbre quedarà així:

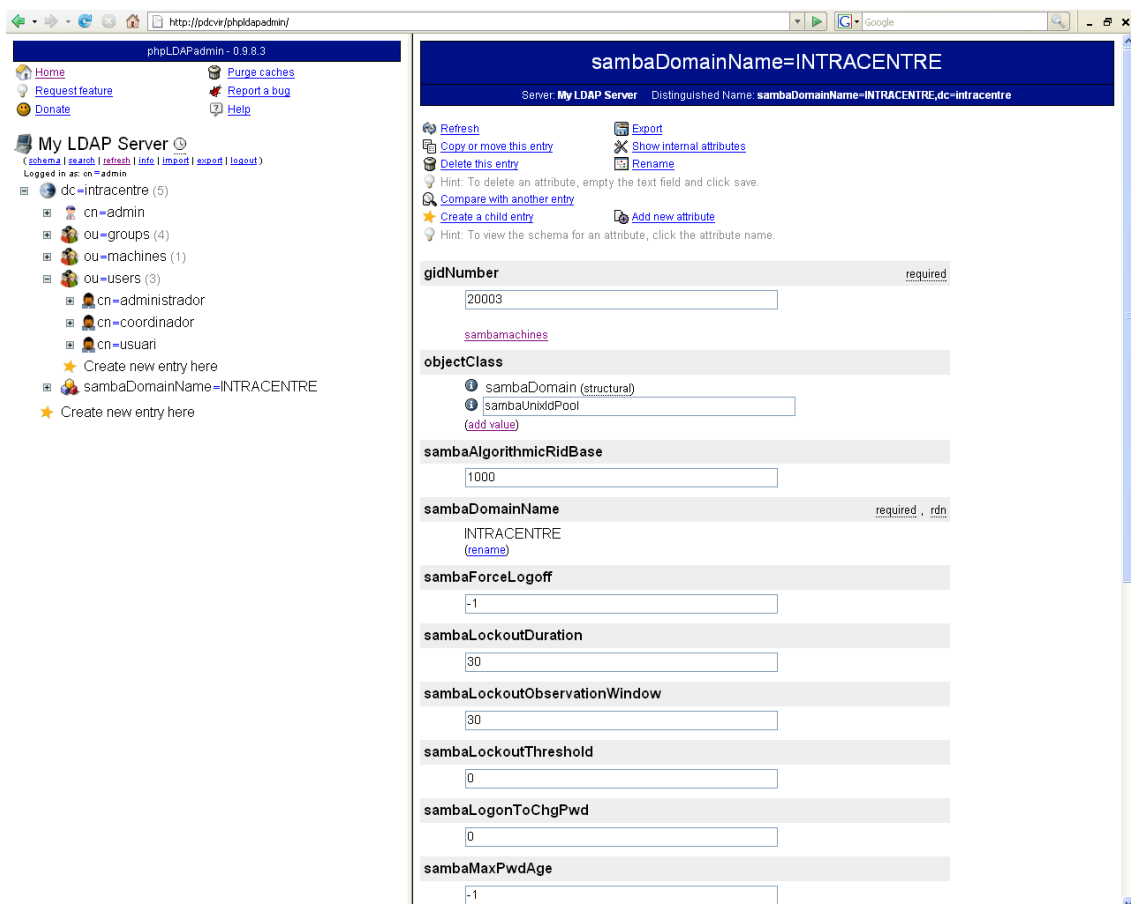


Figura 8: Configuració dels atributs del PDC.

En aquest moment ja podem unir ordinadors al domini i podem anar donant d'alta de forma manual als usuaris que vulguem.

2. Serveis necessaris per a la posada en funcionament del PDC.

- Distribució de Linux Debian Etch.

“Debian o Projecte Debian és una comunitat formada per desenvolupadors i usuaris, que pretén crear i mantenir un sistema operatiu GNU basat en programari lliure precompilat i empaquetat, en un format senzill en múltiples arquitectures d'ordinadors i amb varis nuclis.

Debian va néixer com una aposta per separar en les seves versions el programari lliure del programari no lliure. El model de desenvolupament del projecte és aliè a motius empresarials o comercials, sent portat per davant dels propis usuaris, encara que compta amb l'ajuda de diverses empreses en forma d'infraestructura. Debian no ven directament el seu software, el posa a disposició de qualsevol a Internet, encara que si permet a persones o empreses distribuir comercialment aquest software mentre es respecti la seva llicència.

La comunitat de desenvolupadors de Debian compta amb la representació de *Software in the public Interest*, una organització sense ànim de lucre que dona cobertura legal a diferents projectes de programari lliure.

- Servei SSH

SSH (**S**ecure **S**hell), és el nom d'un protocol i del programa que l'implementa, i serveix per accedir a ordinadors remots a través d'una xarxa. Permet controlar per complet l'ordinador mitjançant un intèrpret de comandes, i també pot redirigir el tràfic de X per a poder executar programes gràfics si tenim un Servidor X executant-se.

A més de la connexió a altres ordinadors, SSH ens permet copiar dades de forma segura (tant fitxers solts com simular sessions FTP xifrades), gestionar claus RSA per no escriure claus al

connectar als ordinadors i passar dades de qualsevol altra aplicació per un canal segur tunelitzat mitjançant SSH.

- Servei Apache

El Servidor Apache és un programari lliure Servidor HTTP de codi obert per a plataformes UNIX (BSD, GNU/Linux, etc.), Windows, Macintosh i altres, que implementa el protocol HTTP/1.1 i la noció de lloc virtual. Quan va començar el seu desenvolupament el 1995 es va basar inicialment en codi del popular NSCA HTTPd 1.3, però més tard fou reescrit per complet. El seu nom es deu a que Behelendorf va escollir el nom perquè volia que tingués connotació d'alguna cosa ferma i enèrgica però no agressiva, i la tribu Apache va ser la última en rendir-se al que aviat es convertiria en govern del EEUU, i en aquells moments la preocupació del seu grup era que arribessin les empreses i “civilitzessin” el paisatge que havien creat els primers enginyers de Internet. A més Apache consistia solament en un conjunt de pedaços a aplicar al servidor NSCA. Era, en anglès, *a patchy server* (un servidor “emparchado”).

El Servidor Apache es desenvolupa dins del projecte HTTP Server (httpd) de la Apache Software Foundation.

- Servei Apache-SSL

Apache-SSL és un servidor web segur, basat en Apache i SSLeay/OpenSSL. Està llicensiat sota la llicència BSD-Style, això significa que, en resum, és lliure i es pot utilitzar tant per usos comercials com no comercials, sempre i quan es conservin els avisos de copyright.

- Servei SAMBA

Samba és una implementació lliure del protocol de fitxers compartits de Microsoft Windows (antigament anomenat SMB, i re nomenat recentment a CIFS) per sistemes de tipus UNIX. D'aquesta forma, es possible que ordinadors amb Linux, Mac OS X o Unix en general es vegin com a servidors o actuïn com clients en xarxes de Windows. Samba també permet validar usuaris fent de Controlador Principal de Domini (PDC), com a membre de domini i inclús com un domini Active Directory per a xarxes basades en Windows; a part de ser capaç de servir cues d'impressió, directoris compartits i autenticar amb el seu propi arxiu de d'usuaris.

Entre els sistemes tipus Unix en els que es pot executar Samba, hi ha les distribucions GNU/Linux, Solaris i les diferents variants BSD entre les que podem trobar Mac OS X Server de Apple.

- Servei LDAP

LDAP (*Lightweight Directory Access Protocol*) és un protocol a nivell d'aplicació que permet l'accés a un servei d'un directori ordenat i distribuït per buscar diversa informació en un entorn de xarxa. LDAP també és considerat una base de dades (encara que el seu sistema d'emmagatzemament pot ser diferents) a la que es poden realitzar consultes.

Habitualment, emmagatzema la informació de login (usuari i contrasenya) i es utilitza per autenticar-se encara que es possible guardar una altra informació (dades de contacte, de l'usuari, ubicació de diversos recursos de la xarxa, permisos, certificats, etc).

En resum, LDAP és un protocol d'accés unificat a un conjunt de informació sobre una xarxa.

- PHPLDAPADMIN

PhpLdapAdmin és una web basada en un client LDAP. Aquest proporciona facilitat, accessibilitat des de qualsevol lloc, i suport multi-idioma per l'administració. El seu arbre jeràrquic i les avançades funcionalitats de cerca el fan intuïtiu per buscar i administrar el directori LDAP. Donat que es tracta d'una aplicació web i que aquest navegador LDAP treballa en moltes plataformes, fa que el servidor sigui fàcil d'administrar des de qualsevol lloc. PhpLdapAdmin és un cercador LDAP perfecte tant per als professionals com per novells. La seva base d'usuaris està formada per professionals de l'administració LDAP.

- Servei MKNTPWD

PhpLdapAdmin requereix una utilitat anomenada MKNTPWD que s'utilitza per a crear el hash de les contrasenyes dels usuaris de Samba. Aquesta funcionalitat hauria d'estar inclosa en el paquet smbldap-tools per no aparèixer inclosa en la Distribució Debian.

- Servei NSS-LDAP

La llibreria nss-ldap permet que un servidor LDAP suplanti als fitxers /etc/passwd, /etc/group i /etc/shadow com a base de dades

del sistema. El seu fitxer de configuració es troba a `/etc/libnss-ldap.conf`.

Posteriorment haurem de configurar el fitxer `/etc/nsswitch.conf` per a que s'utilitzi LDAP com a base de dades del sistema enlloc dels fitxers `passwd`, `group` i `shadow`.

- Servei PAM-LDAP

La llibreria `pam-ldap` permet que les aplicacions que utilitzen PAM per autenticar-se, puguin fer-ho mitjançant un servidor LDAP. Per a que el sistema Linux s'autentifiqui mitjançant un servidor LDAP és necessari instal·lar aquesta llibreria ja que utilitza PAM. El fitxer de configuració d'aquesta llibreria és `/etc/pam_ldap.conf`. Hi ha altres aplicacions o serveis que utilitzen PAM per l'autenticació i per tant podrien, gràcies a la llibreria `pam-ldap`, autenticar-se contra un servidor LDAP.

Per especificar el mètode d'autenticació de cada servei és necessari configurar els fitxers que es troben a la carpeta `/etc/pam.d`.

- Servei NSCD

Per evitar que sigui consulta el servidor LDAP cada cop que s'executi una comanda dins de la nostra organització, es una bona idea configurar als nostres servidors un sistema de cache per algunes dades d'usuari. Mentre les dades en la cache siguin el suficientment recents, les estacions de treball utilitzaran aquestes dades en lloc de preguntar al Servidor LDAP un altre cop. El dimoni servidor de cache de noms (`nscd`) compleix exactament aquestes tasques.

- Servei Smbldap-Tools

`Smbldap-tools` és un conjunt de scripts dissenyats per ajudar en la integració de SAMBA amb el directori LDAP. Està dirigit als usuaris i administradors de Linux, encara que també funciona amb la majoria de sistemes Unix com Solaris o AIX. Els usuaris poden modificar la seva contrasenya de forma similar a la instrucció `passwd`. Els administradors poden administrar als usuaris i grups d'usuaris mitjançant la línia de comandes i sincronitzar els comptes de Samba constantment.

Aquestes eines estan escrites amb Perl, i les podem trobar a Debian a `/usr/share/doc/smbldap-tools/examples`. Es

pot trobar informació sobre l'ús d'aquestes eines, que son simples i directes.

Apartats a configurar per al correcte funcionament. Fitxers de configuració que cal editar per a ficar en funcionament el nostre servidor.

- /etc/libnss-ldap.conf
- /etc/nsswitch.conf
- /etc/pam_ldap.conf
- /etc/pam_ldap.secret
- /etc/ldap/slapd.conf
- /etc/pam.d/common-account
- /etc/pam.d/common-auth
- /etc/pam.d/common-password
- /etc/samba/smb.conf
- /etc/smbldap-tools/smbldap.conf
- /etc/smbldap-tools/smbldap_bind.conf

3. Instal·lació i configuració del sistema de quotes de disc.

Per tal de controlar el volum de les dades dels usuaris s'ha decidit instal·lar el sistema de gestió de quotes de disc. Amb aquest sistema tenim la possibilitat de determinar l'espai de disc dels diferents usuaris de la xarxa i així evitar que determinats usuaris emmagatzemin moltes dades, que a més, normalment no s'adapten ben bé a tasques relacionades amb els estudis o docència.

El sistema de quotes ens permet establir les quotes tant per grup d'usuaris com individualment. En el nostre cas establim les quotes individualment. La configuració per defecte un cop instal·lat el servei estableix una quota de disc il·limitada pels usuaris. En aquest apartat ho deixarem d'aquesta forma, ja que ho deixarem amb la configuració mínima, per ara, per a després administrar el servei mitjançant l'entorn d'administració Webmin (vegeu apartat 7 del capítol 4).

Per instal·lar el sistema de quotes fem el següent:

Aquesta instrucció descarregarà el paquet quota i l'instal·larà al nostre sistema.

```
#apt-get install quota
```

El sistema de quotes treballa amb particions. Per tant, i com que ja hem separat la partició de dades d'usuaris (partició /home) serà aquesta la que configurarem per a posar en funcionament el sistema de quotes. Per seguir amb el procés de configuració cal editar el fitxer fstab situat a: /etc/fstab

El fitxer fstab conté la llista de discs i particions del sistema. En ell s'indica com inicialitzar cada dispositiu i quina configuració utilitzar. En el nostre cas caldrà fer el següent (editar-lo):

```
# /etc/fstab: static file system information.
#
# <file system> <mount point> <type> <options> <dump> <pass>
proc /proc proc defaults 0 0
/dev/hda1 / ext3 defaults,errors=remount-ro 0 1
/dev/hda6 /home ext3 defaults,usrquota,grpquota 0 2
/dev/hda5 none swap sw 0 0
/dev/hdc /media/cdrom0 udf,iso9660 user,noauto 0 0
/dev/fd0 /media/floppy0 auto rw,user,noauto 0 0
```

Figura 9: Contingut del fitxer fstab.

Fixem-nos en la línia:

```
/dev/hda6 /home ext3 defaults,usrquota,grpquota 0 2
```

Cal introduir els paràmetres “usrquota” i “grpquota” per tal d’indicar que en aquesta partició de dades s’utilitzarà el sistema de quotes.

Un cop editat i guardat el fitxer és el moment de tornar a “muntar” la partició de les dades dels usuaris /home:

```
#mount -o remount /home
```

Un cop “re-muntat” el sistema comprovem amb: `mount` que la partició està activada amb `usrquota` i `grpquota`. Ens ha d’aparèixer així:

```

pdc:/home/user# mount
/dev/hda1 on / type ext3 (rw,errors=remount-ro)
tmpfs on /lib/init/rw type tmpfs (rw,nosuid,mode=0755)
proc on /proc type proc (rw,noexec,nosuid,nodev)
sysfs on /sys type sysfs (rw,noexec,nosuid,nodev)
procusb on /proc/bus/usb type usbfs (rw)
udev on /dev type tmpfs (rw,mode=0755)
tmpfs on /dev/shm type tmpfs (rw,nosuid,nodev)
devpts on /dev/pts type devpts (rw,noexec,nosuid,gid=5,mode=620)
/dev/hda6 on /home type ext3 (rw,usrquota,grpquota)
pdc:/home/user#
```

Figura 10: Resultat de la comanda "mount".

Cal crear els fitxers quota.user i quota.group, els quals s'utilitzaran per guardar la informació i l'estat de les quotes en cada partició.

Fem el següent:

```
#touch /home/quota.user
#touch /home/quota.group
#chmod 600 /home/quota.user
#chmod 600 /home/quota.group
```

Ara fem una comprovació preliminar del sistema de quotes amb:

```
#quotacheck -auvg
```

Un cop comprovat el correcte funcionament del servei, l'activem. Els usuaris s'activaran amb quota il·limitada, per tant, podem inicialitzar el servei sense el risc de bloquejar a algun usuari. Per activar el servei:

```
#quotaon -a
```

Amb tot això ja tenim funcionant el sistema de quotes, el qual continuarem administrant des de Webmin.

4. Instal·lació dels serveis per al procés de validació dels usuaris wi-fi.

A més del PDC també necessitem instal·lar un altre servei al nostre Servidor per tal de poder realitzar les autenticacions dels usuaris wi-fi. El

servei que ens permet realitzar aquestes autenticacions és el Servei RADIUS. En el nostre servidor instal·larem el servei de codi obert “FreeRadius”.

“**RADIUS** (acrònim en Inglés de *Remote Authentication Dial-In User Server*).

És un protocol d'autenticació i autorització per aplicacions d'accés a la xarxa o mobilitat IP. Utilitza el port 1813 UDP per establir les seves connexions.

Quan es realitza la connexió amb un ISP [7] mitjançant mòdem, DSL, cablemodem, Ethernet o Wi-Fi, s'envia una informació que generalment es un nom d'usuari i una contrasenya. Aquesta informació es transfereix a un dispositiu NAS (Servidor d'accés a la xarxa) sobre el protocol PPP, que redirigeix la petició a un servidor RADIUS sobre el protocol RADIUS. El servidor RADIUS comprova que la informació és correcta utilitzant esquemes d'autenticació com PAP [8], CHAP [9] o EAP [10]. Si és acceptat, el servidor autoritzarà l'accés al sistema ISP i li assignarà els recursos de xarxa com la direcció IP, i altres paràmetres com L2TP [11], etc.

Una de les característiques més importants del protocol RADIUS és la seva capacitat de controlar sessions, notificant quan comença i acaba una connexió, així que a l'usuari se li podrà determinar el seu consum i facturar en conseqüència; les dades es poden utilitzar amb propòsits estadístics.

RADIUS va ser desenvolupat originalment per Livingston Enterprises per la sèrie PortMaster dels seus serveis d'accés a la xarxa, més tard es va publicar com RFC 2138 i RFC 2139. Actualment existeixen molts servidors RADIUS, tant comercials com de codi obert. Les prestacions poden variar, però la majoria poden gestionar els usuaris en arxius de text, servidor LDAP, bases de dades variades, etc. Sovint s'utilitza SNMP per controlar remotament el servei. Els servidors Proxy RADIUS s'utilitzen per una administració centralitzada poden reescriure paquets RADIUS al aire (per motius de seguretat, o fer conversions entre dialectes de diferents fabricants).”

Per tal d'instal·lar el servei necessitem instal·lar el paquets de Debian: freeradius i freeradius-ldap.

#apt-get install freeradius freeradius-ldap

Es descarregaran els paquets i s'instal·laran en el nostre servidor. Un cop instal·lat el servei ara és el moment d'establir els paràmetres de configuració amb l'objectiu de que aquest servei pugui realitzar les consultes a la base de dades LDAP que tenim instal·lada fins al moment.

Ens situem dins el directori on hi ha els fitxers de configuració del servei RADIUS.

```
#cd /etc/freeradius
```

Un cop dins el directori, utilitzem el editor vim per modificar la configuració inicial .

```
#vi m radius.conf
```

El fitxer ha de contenir la següent configuració.

```
ldap {
    server = "localhost"
    identity = "cn=admin,dc=intracentre"
    password = password
    basedn = "dc=intracentre"
    filter = "(uid=%u)"
    start_tls = no
    access_attr = "uid"
    dictionary_mapping = ${raddbdir}/ldap.attrmap
    ldap_connections_number = 5
    timeout = 4
    timelimit = 3
    net_timeout = 1
}
```

Cal buscar la línia de configuració que conté:

```
#ldap
```

I des comentar aquesta opció per tal d'activar la possibilitat de realitzar validacions contra el nostre servei LDAP

Per últim, en el mateix fitxer també cal des comentar l'apartat:

```
# Auth-Type LDAP {
#     ldap
# }
```

Cal també editar el fitxer users.

```
#vi m users
```

Busquem el text:

```
DEFAULT Auth-Type = System
Fall-Through = 1
```

I el substituïm per:

```
DEFAULT Auth-Type = LDAP
```

Fall-Through := 1

Per últim, editem el fitxer clients.conf. En aquest fitxer es defineixen els dispositius que interactuaran amb el servei RADIUS i la contrasenya que s'intercanviaran. Per provar la correcta instal·lació del servei ens servirà l'opció que ve per defecte:

```
#vim clients.conf
```

```
client 127.0.0.1 {
    secret          = testing123
    shortname       = localhost
    nastype         = other
}
```

Comprovació del correcte funcionament. Primerament reiniciem el servei per a que s'estableixi amb els paràmetres introduïts anteriorment.

```
#/etc/init.d/freeradius restart
```

Llencem el programa per "testejar" el correcte funcionament del servei. Caldrà tenir creat un usuari a la nostra base de dades. Ho provem de forma local.

```
#radtest usuari passwordusuari 127.0.0.1 0 testing123
```

Si tot va bé ens apareixerà:

```
Sending Access-Request of id 229 to 127.0.0.1 port
1812
    User-Name = "usuari "
    User-Password = "passwordusuari "
    NAS-IP-Address = 255.255.255.255
    NAS-Port = 0
rad_recv: Access-Accept packed from host
127.0.0.1: 1812, id=229, length=20
```

En cas contrari el missatge serà:

```
Sending Access-Request of id 229 to 127.0.0.1 port
1812
    User-Name = "usuari "
    User-Password = "password"
    NAS-IP-Address = 255.255.255.255
    NAS-Port = 0
rad_recv: Access-Reject packed from host
127.0.0.1: 1812, id=229, length=20
```

Un cop comprovat el correcte funcionament, donem d'alta els dispositius (clients) que realitzaran processos de validació contra el Servei RADIUS instal·lat al PDC.

En el nostre cas caldrà donar d'alta (indicar la direcció IP) l'ordinador on està instal·lat el Portal Captiu. La direcció IP d'aquest ordinador és: 192.168.3.1 i el password que utilitzarem és: passwordportal. Per tant, afegirem la següent configuració dins el fitxer users del directori del freeradius:

```
client 192.168.3.1 {  
    secret           = passwordportal  
    shortname       = portal  
    nastype         = other  
}
```

Fitxers de configuració que cal editar per ficar en funcionament el Servei RADIUS (FreeRadius).

- /etc/freeradius/radiusd.conf
- /etc/freeradius/clients.conf
- /etc/freeradius/users

En aquest moment ja estem en disposició d'utilitzar el Servei RADIUS per a poder realitzar les autenticacions del usuaris de la xarxa wi-fi.

5. Extracció dels fitxers de configuració.

Un cop ja tenim el servidor configurat, seria adequat realitzar una copia de seguretat dels fitxers que hem modificat per tal de ficar en funcionament el servidor.

Aquesta copia ens pot ser de gran ajuda en cas de fallida del sistema ja que ens aportaria facilitat i rapidesa a l'hora de restablir el sistema. No ens faria falta editar els fitxers de configuració, senzillament, sobreescrivint el fitxer i reiniciant el servei n'hauria prou per restablir els serveis instal·lats al servidor.

El Backup el podem realitzar directament des del Servidor seleccionant els fitxers de configuració o també ho podríem fer de forma remota, utilitzant aplicacions que ens poden automatitzar molt aquest procés.

Tant si utilitzem Windows com Linux trobem com a mínim dues aplicacions que ens permeten realitzar aquest Backup de forma remota.

Per Windows tenim el WinSCP. "WinSCP és una aplicació de Software Lliure. WinSCP és un client SFTP [12] gràfic per Windows que utilitza SSH. L'anterior protocol SCP també es pot utilitzar. La seva funció

principal es facilitar la transferència segura de fitxers entre dos sistemes informàtics, el local i un de remot que ofereixi serveis SSH.”

Per tal d’iniciar la copia de fitxers, iniciarem el programa, introduïrem la direcció IP del Servidor PDC juntament amb les dades del administrador del PDC. Les dades seran:

IP o nom: 192.168.0.11 o pdc

Usuari: root

Contrasenya: password

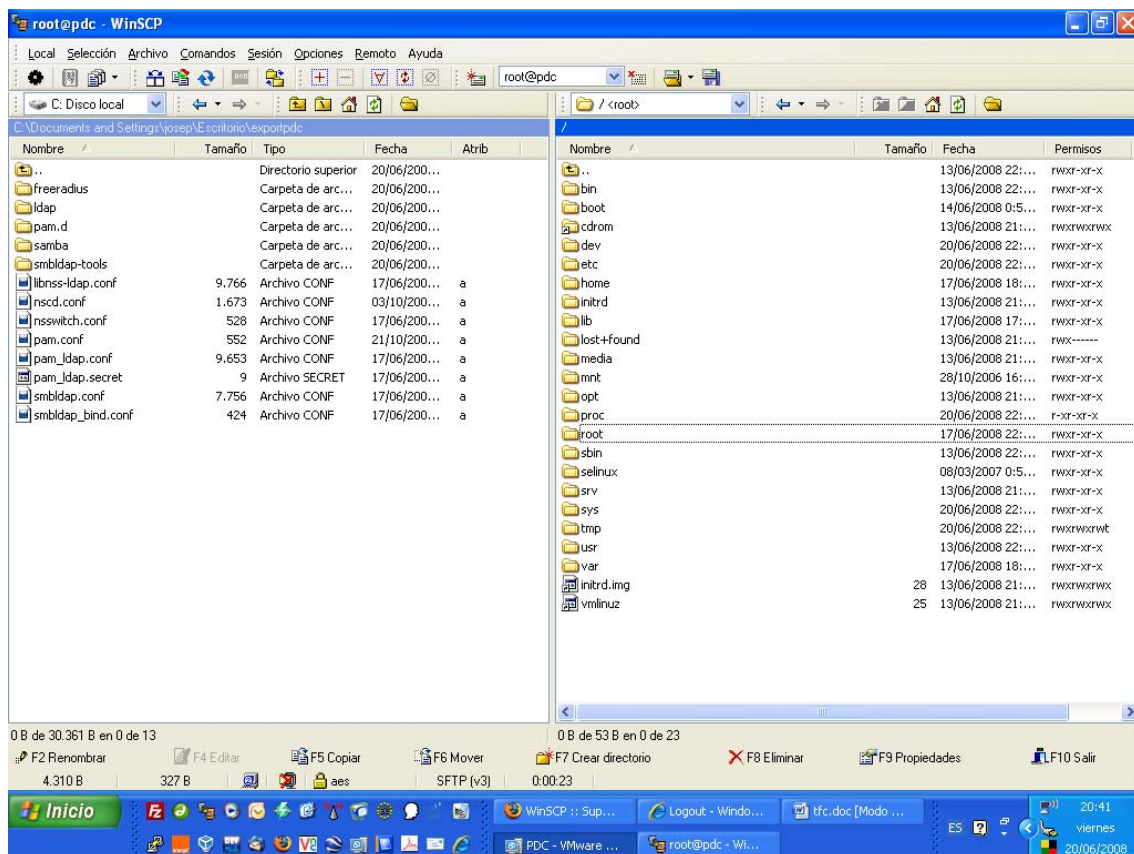


Figura 11: Exportació de fitxers des de WinSCP i Windows.

Per Linux, en el nostre cas Kubuntu (Sistema operatiu Ubuntu amb entorn gràfic KDE [13]), utilitzarem el navegador “Konqueror” ja que aquest ja porta incorporat el client SFTP.

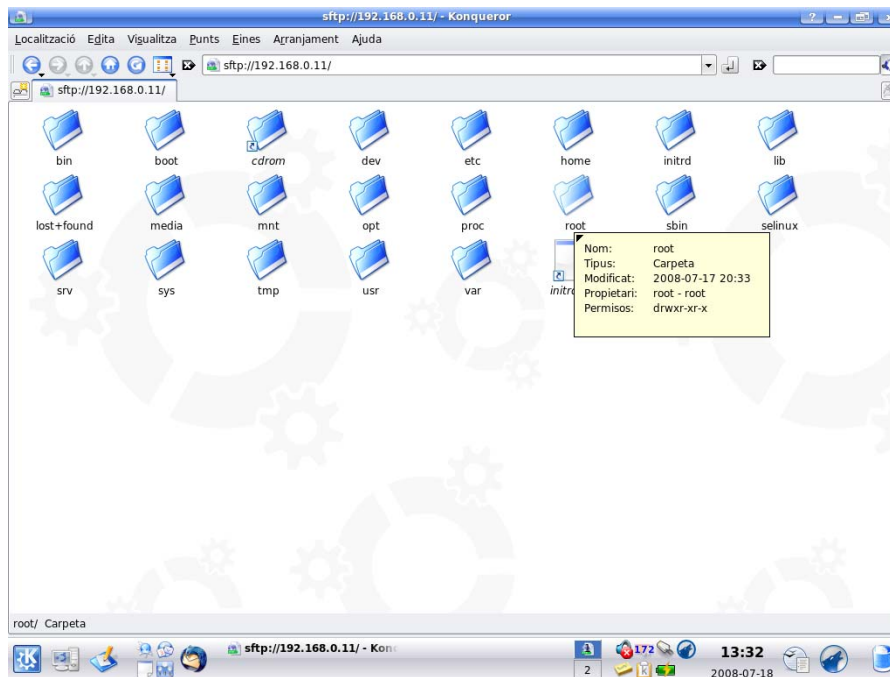


Figura 12: Exportació de fitxers des de Konqueror i Kubuntu.

Per tal de realitzar el Backup des de Kubuntu iniciarem el konqueror i escriurem a la barra d'adreces:

sftp://192.168.0.11

Se'ns demanarà el nom d'usuari i contrasenya. Introduïrem les mateixes dades que des del Winscp:

Usuari: root

Contrasenya: password

6. Backup del PDC.

Pel que fa a les còpies de seguretat s'han estat provant diferents alternatives.

Des d'un principi es va pensar en la possibilitat de configurar un altre servidor PDC, en aquest seria un BDC (Back Up Domain Controller) per tal de tenir una còpia exacta del PDC i a més un ordinador capaç de respondre com a PDC en cas de fallida del PDC inicial. Aquesta opció però, es va desestimar ja que el centre no volia tenir un altre ordinador destinat a aquesta finalitat, i a més, el fet de tenir un altre ordinador amb la complexitat del PDC dificultava la gestió de tot el sistema.

La segona opció va ser la de configurar un servidor de dades extern. Un ordinador molt menys complex i amb uns objectius més reduïts. Aquest ordinador seria molt fàcil d'administrar ja que només tindria a com a objectiu emmagatzemar les còpies de seguretat dels usuaris. Es va pensar en un Sistema NAS (Network-Attached Storage), emmagatzematge connectat en xarxa. Concretament es va provar el software FreeNAS, un sistema operatiu basat en FreeBSD.

Aquest sistema operatiu gratuït, i de lliure distribució, permet convertir un ordinador personal en un suport de emmagatzematge accessible des de la xarxa, per exemple emmagatzematge massiu, d'informació, Backup, etc..

Característiques del servidor FreeNAS:

- Tamany reduït (menys de 32 Mb)
- Fàcil i ràpida instal·lació. Molt semblant al Pfsense ja que es basen en la mateixa distribució.
- Requisits del sistema molt baix.
- Fàcil administració remota, a través d'una pàgina web accessible des de qualsevol ordinador de la xarxa mitjançant un navegador.
- No es necessari tenir connectat un monitor ni teclat per al seu funcionament.
- Es pot instal·lar en diferents suports, USB, disc dur, o targeta CompactFlash.
- RAID [14] Hardware i Software.

Tot i les característiques que presenta es va acabar desestimant per dos motius, un era que aquest software encara es troba en fase de desenvolupament i l'altra, que necessitem un altre ordinador en funcionament. Val a dir però, que en un futur es tornarà a valorar aquest solució ja que de ben segur s'haurà avançat molt en aquest software i a més ens aportarà noves funcionalitats interessants.

Per últim s'ha decidit utilitzar un disc dur USB extern connectat al PDC. Es tracta de la solució més barata de totes i també la menys complexa. Només cal connectar el disc al PDC i configurar el programa de Back Up (Rsync) per que guardi les còpies de seguretat en aquest disc dur.

Rsync és una aplicació per sistemes tipus UNIX que ofereix transmissions eficients de dades incrementals comprimides i xifrades. Mitjançant una tècnica de compressió de fitxers, permet sincronitzar fitxers i directoris entre dues màquines d'una xarxa o entre dues ubicacions en una mateixa màquina, minimitzant el volum de dades transferides.

Pel que fa la copia de seguretat del sistema cal valorar de quins directoris del PDC cal realitzar una copia de seguretat. En apartats anteriors ja hem explicat com realitzar una copia dels fitxers de configuració dels serveis, per tant, ara ens centrarem en realitzar, només, la copia de seguretat dels fitxers dels usuaris donats d'alta al sistema, és a dir, el directori **/home** del PDC.

Les còpies de seguretat que realitzarem no les farem com a administradors del servidor, sinó com a usuaris "normals", ja que d'aquesta manera farem més fàcil la restauració dels fitxers en cas de fallida.

Per començar a realitzar la copia de seguretat el sistema necessitem:

- Instalar el servei rsync amb: **#apt-get install rsync**
- Connectar el nostre disc dur al PDC i engegar-lo.
- Comprovem amb l'usuari root en quina unitat ha estat connectat el nostre disc dur extern. Ho fem a la instrucció:

#tail -f /var/log/messages

```
pdc:/# tail -f /var/log/messages
Sep 1 07:50:37 pdc kernel: SCSI device sda: 78165360 512-byte hdwr sectors (40021 MB)
Sep 1 07:50:37 pdc kernel: sda: Write Protect is off
Sep 1 07:50:37 pdc kernel: SCSI device sda: 78165360 512-byte hdwr sectors (40021 MB)
Sep 1 07:50:37 pdc kernel: sda: Write Protect is off
Sep 1 07:50:37 pdc kernel: sda: sda1
Sep 1 07:50:37 pdc kernel: sd 5:0:0:0: Attached scsi disk sda
Sep 1 07:52:06 pdc kernel: usb 5-4: USB disconnect, address 5
Sep 1 07:52:20 pdc kernel: usb 5-4: new high speed USB device using ehci_hcd and address 6
Sep 1 07:52:20 pdc kernel: usb 5-4: configuration #1 chosen from 1 choice
Sep 1 07:52:20 pdc kernel: scsi6 : SCSI emulation for USB Mass Storage devices
Sep 1 07:52:25 pdc kernel: Vendor: WDC WD40 Model: OEB-75CPFO Rev: 0000
Sep 1 07:52:25 pdc kernel: Type: Direct-Access ANSI SCSI revision: 00
Sep 1 07:52:25 pdc kernel: SCSI device sda: 78165360 512-byte hdwr sectors (40021 MB)
Sep 1 07:52:25 pdc kernel: sda: Write Protect is off
Sep 1 07:52:25 pdc kernel: SCSI device sda: 78165360 512-byte hdwr sectors (40021 MB)
Sep 1 07:52:25 pdc kernel: sda: Write Protect is off
Sep 1 07:52:25 pdc kernel: sda: sda1
Sep 1 07:52:25 pdc kernel: sd 6:0:0:0: Attached scsi disk sda
```

Figura 13: Reconeixement dels disc extern.

Veiem que el nostre disc USB es presenta com una unitat SCSI a `/dev/sda` en la partició `/dev/sda1`.

Premem: `Ctrl + C` per sortir de la comanda `tail`

El sistema de fitxers del nostre disc dur USB serà EXT3. Ara cal editar el fitxer: `/etc/fstab` per tal de poder-hi accedir.

```
# /etc/fstab: static file system information.
#
# <file system> <mount point> <type> <options> <dump> <pass>
proc /proc proc defaults 0 0
/dev/hda1 / ext3 defaults,errors=remount-ro 0 1
/dev/hda6 /home ext3 defaults,usrquota,grpquota 0 2
/dev/hda5 none swap sw 0 0
/dev/hdc /media/cdrom0 udf,iso9660 user,noauto 0 0
/dev/fd0 /media/floppy0 auto rw,user,noauto 0 0
/dev/sda1 /mnt/usb ext3 user,noauto,rw 0 0
```

Figura 14: Edició del fitxer `/etc/fstab`

Les opcions establertes signifiquen que qualsevol usuari pot muntar el sistema de fitxers, però que només l'usuari que ha muntat el sistema de fitxers pot desmuntar-lo (`user`), el sistema de fitxers no es muntarà al iniciar el ordinador (`noauto`), i el sistema de fitxers es muntarà amb permisos de lectura i escriptura (`rw`).

Creem el directori “usb” dins de `/mnt`:

```
#mkdir /mnt/usb
```

I montem el disc USB extern a la partició creada amb:

```
#mount /dev/sda1 /mnt/usb
```

Ara podem provar el disc dur com a un usuari “normal”:

```
#mount /mnt/usb
```

```
#df -k
```

Ens retornarà:

```
pdc:/# df -k
S. fitxers      Blocs    1K      Usats    Lliures  %ús Muntat en
/dev/hda1      6728280 3654292 2732208 58% /
tmpfs          257668  0      257668  0% /lib/init/rw
udev           10240   64     10176  1% /dev
tmpfs          257668  0      257668  0% /dev/shm
/dev/hda6      30352332 200504 28609992 1% /home
/dev/sda1      38769320 206916 36608500 1% /mnt/usb
pdc:/#
```

Figura 15: Muntat del disc extern.

Per tal de tenir millor organitzat el sistema de còpies de seguretat podem crear un directori anomenat backup. Per crear-lo fem:

```
#mkdir /mnt/usb/backup
```

Per deixar més clar encara de quin ordinador fem el Backup podem crear una carpeta dins del directori de Backup amb el nom de l'ordinador del qual farem el Backup, en el nostre cas del PDC. Per tant, fem el següent:

```
#mkdir /mnt/usb/backup/pdc
```

Realització del Backup:

Per tal de realitzar un Backup de tota el directory /home del nostre PDC caldrà executar la següent comanda:

```
#rsync -vrlptg /home/ /mnt/usb/backup/pdc/home
```

Els paràmetres utilitzats amb rsync són:

- v verbose output
- r recursivitat dins dels directoris
- l copiar enllaços simbòlics com enllaços simbòlics.
- p conserva els permissos
- t conserva l'hora
- g conserva el grup

Restauració dels fitxers:

En el cas de que el disc del pdc és fes malbé o passes qualsevol altra desgracia podríem restaurar els fitxers dels directoris dels usuaris d'una forma molt semblant a la de la creació del Backup.

```
#rsync -vrlptg /mnt/usb/backup/pdc/home /home
```

Automatització del Backup:

Per automatitzar les còpies de seguretat del nostre PDC utilitzarem l'administrador regular de processos "cron" [28]. Aquest però, l'administrarem des de l'entorn d'administració Webmin (vegeu apartat 7

del capítol 4). A través de Webmin ens serà molt més fàcil indicar quan volem que es realitzin les còpies de seguretat del nostre PDC.

Una possible configuració del cron amb Webmin seria:

Edició de Treball Cron

Detalls del treball

Executa el treball cron com:

Activa: ☒ Sí ☐ No

Ordre:

Entrada de l'ordre:

Descripció:

Temps d'execució

☐ Planificació simple... ☒ Hores i dates seleccionades a sota...

Minuts

☐ Tots ☒ Seleccionats ...

0	1	2	3	4	5	6	7	8	9	10	11
12	13	14	15	16	17	18	19	20	21	22	23
24	25	26	27	28	29	30	31	32	33	34	35
36	37	38	39	40	41	42	43	44	45	46	47
48	49	50	51	52	53	54	55	56	57	58	59

Hores

☐ Tots ☒ Seleccionats

0	1	2	3	4	5	6	7	8	9	10	11
12	13	14	15	16	17	18	19	20	21	22	23

Dies

☒ Tots ☐ Seleccionats ...

1	2	3	4	5	6	7	8	9	10	11	12
13	14	15	16	17	18	19	20	21	22	23	24
25	26	27	28	29	30	31					

Mesos

☒ Tots ☐ Seleccionats

Gener	Febrer	Març	Abril	Maig	Juny	Juliol	Agost	Setembre	Octubre	Novembre	Desembre
-------	--------	------	-------	------	------	--------	-------	----------	---------	----------	----------

Dies de la Setmana

☐ Tots ☒ Seleccionats

Dilluns	Dimarts	Dimecres	Dijous	Divendres	Dissabte	Diumenge
---------	---------	----------	--------	-----------	----------	----------

Nota: Fes Ctrl-clic (o command-click al Mac) per a seleccionar i deseleccionar minuts, hores, dies i mesos.

Interval de dates d'execució

☒ Executa'l qualsevol dia ☐ Executa'l només des de / / fins a / /

Figura 16: Configuració de rsync amb cron i Webmin.

Aquesta configuració de cron triada ens executarà la comanda rsync cada dia a la mateixa hora els dies de la setmana que hem triat, de dilluns a divendres.

7. Instal·lació i administració del servidor amb Webmin.

Webmin es defineix com “una interfície que permet administrar sistemes UNIX utilitzant un navegador web que suporti taules i formularis. Webmin permet, per exemple, administrar els comptes d'usuari, Apache, DNS, Samba, DHCP, compartir fitxers, apagar l'ordinador, tot això des d'una interfície web fàcil d'utilitzar.”

En el nostre cas, Webmin ens permetrà controlar el Servidor PDC des de qualsevol màquina de la xarxa de forma remota. Per controlar, el servei LDAP ja utilitzem el PhpLDAPadmin com a Front-end, però per controlar

remotament la resta de serveis havíem d'utilitzar, fins al moment, només connexions ssh. Per tant el fet d'administrar el servidor des d'un entorn web ens facilitarà i molt les tasques d'administració i manteniment del nostre Servidor PDC.

Entre aquestes tasques es troba per exemple el sistema de quotes de disc dels usuaris o el sistema de còpies de seguretat dels usuaris (Rsync). A més, Webmin té suport per a l'administració dels molts serveis, la qual cosa, fa que sigui una eina molt potent i fàcil que ens permetrà ampliar els serveis de forma fàcil i còmoda.

Per instal·lar el Webmin necessitem descarregar-nos el paquet des de seva pàgina oficial, en el nostre cas, serà un fitxer .deb ja que estem utilitzant la distribució Debian. Des de la consola podem fer:

```
#wget  
http://prdownloads.sourceforge.net/webadmin/webmin\_1.420\_all.deb
```

Aquest paquet però, depèn d'altres paquets (dependències) que cal tenir instal·lats. Aquests paquets ja estan dins dels repositoris de Debian, per tant, podem instal·lar-los de la següent forma:

```
#apt-get install openssl libnet-ssl-eay-perl  
libauthen-pam-perl libio-pty-perl libmd5-perl
```

Un cop instal·lats aquests paquets podem seguir instal·lant el Webmin. Ens situem al directori on l'hem descarregat i fem:

```
#dpkg -i webmin_1.420_all.deb
```

Un cop instal·lat ja podem accedir a administrar el Servidor PDC des d'un entorn web. Per fer-ho, obrirem el navegador i ficarem l'adreça següent:

```
https://pdc:10000
```

Acceptem els certificats, introduïm les credencials de l'usuari root de l'ordinador i ja podem començar a administrar el nostre servidor.

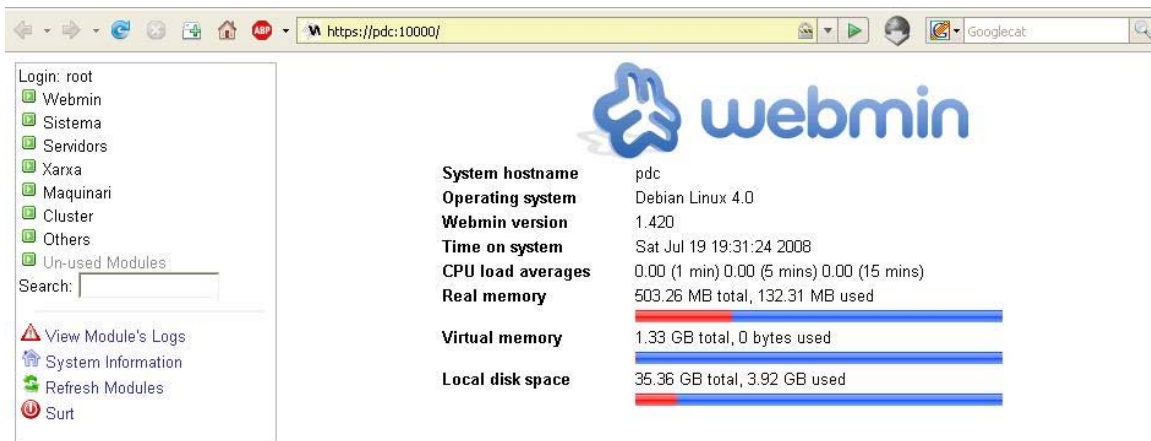


Figura 17: Pantalla principal de Webmin.

Capítol 5: Instal·lació del Portal captiu.

1. Instal·lació de Pfsense.

Tal i com hem comentat en els capítols anteriors (capítol 2), el programari que utilitzarem per a ficar en funcionament el Portal captiu és el Pfsense. Aquest software no necessitarà un ordinador molt potent per a funcionar de forma optima, per aquest motiu podríem utilitzar un ordinador dels que disposa el centre i que actualment no està en funcionament. En aquest cas l'ordinador haurà de disposar de dues targetes de xarxa, una que actuarà com a porta d'enllaç del Portal captiu (WAN) [15], i l'altra que escoltarà les peticions del usuaris wi-fi que vulguin connectar-se a la xarxa sense fils (LAN) [16]. Un cop descarregada la versió ISO del PfSense (també es pot descarregar la versió Embedded [17] per a poder instal·lar PfSense en una memòria compact flash) la gravem en un cd, arranquem l'ordinador des de l'unitat de cd-rom i seguim els passos d'instal·lació que ens marca l'assistent.

Com que primer hem arrencat el servidor des de Live cd, el primer que haurem de fer és instal·lar el software al ordinador. Per tant, seguint l'assistent instal·lem el Pfsense al disc dur de l'ordinador.



Figura 18: Pantalla de benvinguda de l'instal·lador de FreeBSD.

La Figura 5.1 mostra la pantalla inicial que ens trobem quan iniciem amb el Live CD del Pfsense. Es tracta del gestor d'arrencada del Sistema Operatiu Free BSD. En el nostre cas arrancarem amb l'opció 1: " Boot Free BSD [default]".

```
Generating MFS /etc partition
Generating MFS /root partition
Looking for pfi.conf on acd0c done.
Looking for pfi.conf on fd0 done.
Looking for config.xml on fd0 done.
Generating a MFS /conf partition... done.
Mounting filesystems... done.
Creating symlinks.....done.
Launching PHP init system... done.
Initializing..... done.
Starting device manager (devd)...done.
Loading configuration.....done.

Network interface Mismatch -- Running interface assignment option.

Valid interfaces are:

le0      00:0c:29:c6:50:57
le1      00:0c:29:c6:50:61

Do you want to set up VLANs first?
If you are not going to use VLANs, or only for optional interfaces, you should
say no here and use the webConfigurator to configure VLANs later, if required.

Do you want to set up VLANs now [y|n]? █
```

Figura 19: Creació de VLAN.

En la figura 5.2 se'ns pregunta si volem configurar VLANs en aquest moment. Per ara li diem que no (introduint "n" seguit de "Enter". Aquesta opció sempre es pot utilitzar un cop ja tinguem el Pfsense instal·lat en el nostre ordinador.

```

Network interface mismatch -- Running interface assignment option.

Valid interfaces are:

le0      00:0c:29:c6:50:57
le1      00:0c:29:c6:50:61

Do you want to set up VLANs first?
If you are not going to use VLANs, or only for optional interfaces, you should
say no here and use the webConfigurator to configure VLANs later, if required.

Do you want to set up VLANs now [y!n]?n

*NOTE*  pfSense requires *AT LEAST* 2 assigned interfaces to function.
        If you do not have two interfaces you CANNOT continue.

        If you do not have at least two *REAL* network interface cards
        or one interface with multiple VLANs then pfSense *WILL NOT*
        function correctly.

If you do not know the names of your interfaces, you may choose to use
auto-detection. In that case, disconnect all interfaces now before
hitting 'a' to initiate auto detection.

Enter the LAN interface name or 'a' for auto-detection: █

```

Figura 20: Configuració de les interfícies de xarxa (LAN).

En aquest pas de la instal·lació hem de determinar el rol de les interfícies de xarxa que l'instal·lador ha detectat. Per tal de fer-ho fàcil, interpretarem la interfície que acaba amb "0" (le0) com la interfície que actua com a WAN, basant-nos en que el "0" l'interpretem com "out" (extern). Fem quelcom similar amb la interfície acabada amb "1" (le1) com la interfície que actua com a LAN, basant-nos en que "1" l'interpretem com "in" (intern).

```

Valid interfaces are:

le0      00:0c:29:c6:50:57
le1      00:0c:29:c6:50:61

Do you want to set up VLANs first?
If you are not going to use VLANs, or only for optional interfaces, you should
say no here and use the webConfigurator to configure VLANs later, if required.

Do you want to set up VLANs now [y!n]?n

*NOTE*  pfSense requires *AT LEAST* 2 assigned interfaces to function.
        If you do not have two interfaces you CANNOT continue.

        If you do not have at least two *REAL* network interface cards
        or one interface with multiple VLANs then pfSense *WILL NOT*
        function correctly.

If you do not know the names of your interfaces, you may choose to use
auto-detection. In that case, disconnect all interfaces now before
hitting 'a' to initiate auto detection.

Enter the LAN interface name or 'a' for auto-detection: le1

Enter the WAN interface name or 'a' for auto-detection: le0 █

```

Figura 21: Configuració de les interfícies de xarxa (WAN).

Determinem el rol de cada interfície.


```

*NOTE*  pfSense requires *AT LEAST* 2 assigned interfaces to function.
        If you do not have two interfaces you CANNOT continue.

        If you do not have at least two *REAL* network interface cards
        or one interface with multiple VLANs then pfSense *WILL NOT*
        function correctly.

        If you do not know the names of your interfaces, you may choose to use
        auto-detection. In that case, disconnect all interfaces now before
        hitting 'a' to initiate auto detection.

        Enter the LAN interface name or 'a' for auto-detection: le1

        Enter the WAN interface name or 'a' for auto-detection: le0

        Enter the Optional 1 interface name or 'a' for auto-detection
        (or nothing if finished):

        The interfaces will be assigned as follows:

        LAN   -> le1
        WAN   -> le0

        Do you want to proceed [y\!n]?

```

Figura 22: Confirmació de la configuració escollida.

Un cop escollida la configuració ens demana de confirmar la informació introduïda en els passos anteriors. Li diem “y” (yes) seguit de enter.

```

*** Welcome to pfSense 1.2-RELEASE-cdrom on pfSense ***

WAN*          ->   le0          ->   172.16.1.234(DHCP)
LAN*          ->   le1          ->   192.168.1.1

pfSense console setup
*****
0) Logout (SSH only)
1) Assign Interfaces
2) Set LAN IP address
3) Reset webConfigurator password
4) Reset to factory defaults
5) Reboot system
6) Halt system
7) Ping host
8) Shell
9) PFtop
10) Filter Logs
11) Restart webConfigurator
12) pfSense PHP shell
13) Upgrade from console
99) Install pfSense to a hard drive/memory drive, etc.

Enter an option: 99

```

Figura 23: Instal·lar el sistema al Disc dur de l'ordinador.

La figura ens mostra la “Consola de configuració inicial”. A través d’ella podrem administrar l’aplicació, ja sigui triant les opcions mostrades, o entrant a la Shell (opció 8) per a configuracions més precises.

En aquest moment ja podríem començar a utilitzar el Pfsense des de el Live CD. Podríem començar per determinar la direcció IP de la Interfície que actua com LAN. Un cop escollida, des d’un navegador web ja podríem introduir la direcció IP de la LAN escollida i començar a configurar el nostre HotSpot (en el cas de l’exemple introduiríem la direcció IP: 192.168.1.1).

En el nostre cas el que ens interessa no es treballar amb l’aplicació des de Live CD, sinó que volem que el Portal captiu estigui instal·lat en el disc dur de l’ordinador on configurarem el Portal captiu. Per portar a terme aquesta opció introduïrem l’opció 99 i seguirem els pasos d’instal·lació.



Figura 24: Confirmació de la configuració de l'entorn triada.

En aquest apartat podrem escollir la configuració amb a la qual s’instal·larà el Pfsense al nostre ordinador, com per exemple la configuració de la tarja gràfica, la resolució o la configuració de teclat. En el nostre cas acceptem el que venen per defecte seleccionant l’opció “Accept these settings”.

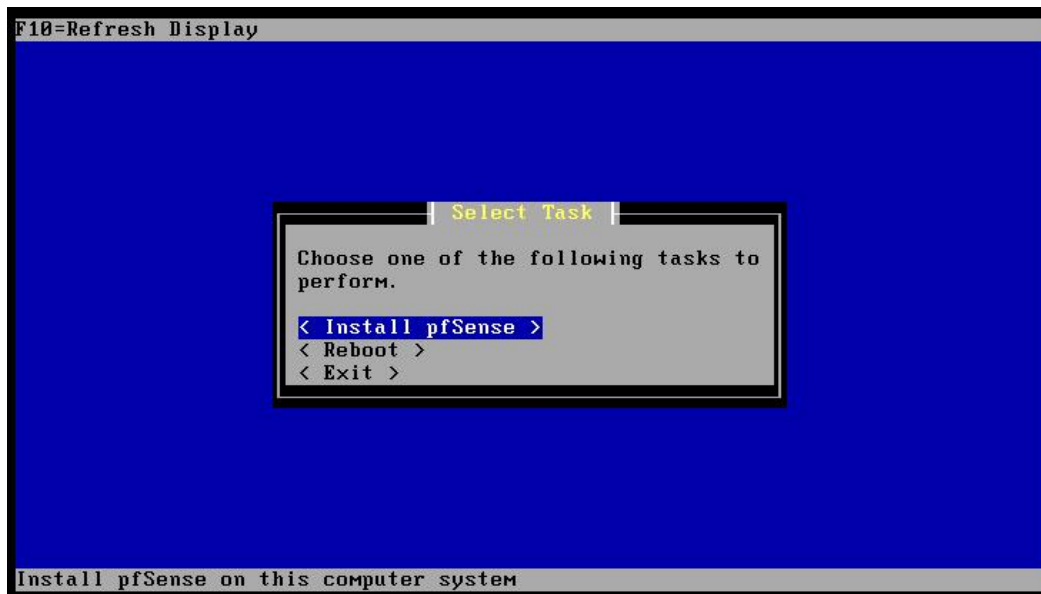


Figura 25: Començament del procés d'instal·lació.

En aquest apartat escollim el pas que volem fer. És a dir, continuar amb la instal·lació del Pfsense, reiniciar el ordinador o sortir (tornant a la consola de configuració inicial). Seleccionem "Install PfSense".

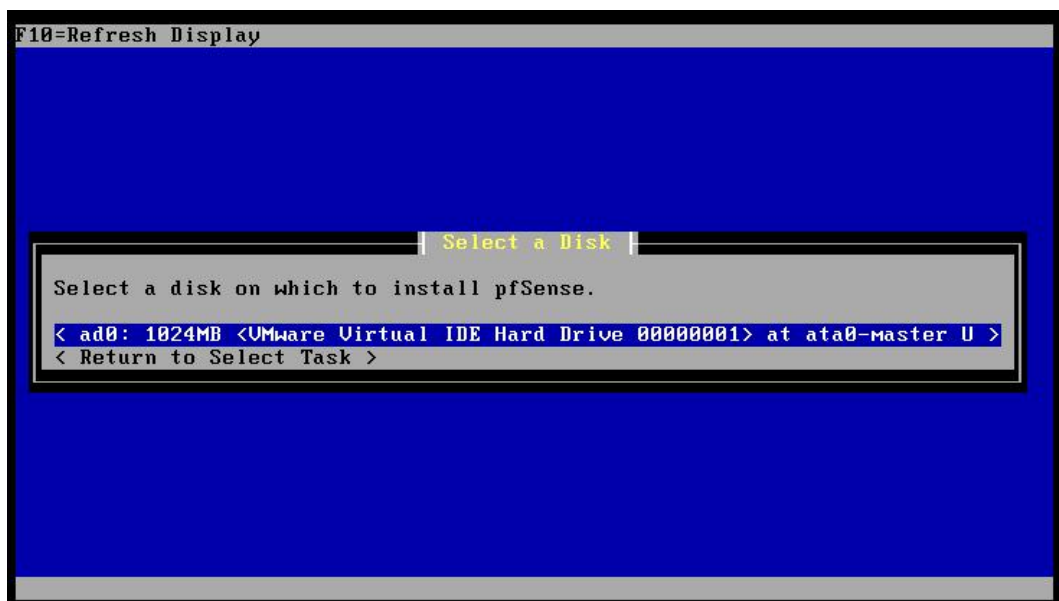


Figura 26: Selecció del disc on s'instal·larà el sistema.

Seleccionem el disc dur on s'instal·larà el PfSense. En la imatge es mostra un disc dur virtual creat amb el VMware. En un cas real la imatge serà similar. Si el disc és IDE, per defecte es mostrarà com "ad0". Seleccionem l'opció marcada amb "Enter".



Figura 27: Formatació del disc.

En aquest punt se'ns dona la possibilitat de formatar el disc dur. És recomanable fer-ho, ja que ens assegurem de que el disc està malmès o conté sectors defectuosos. Seleccionem l'opció de "Format this Disk".

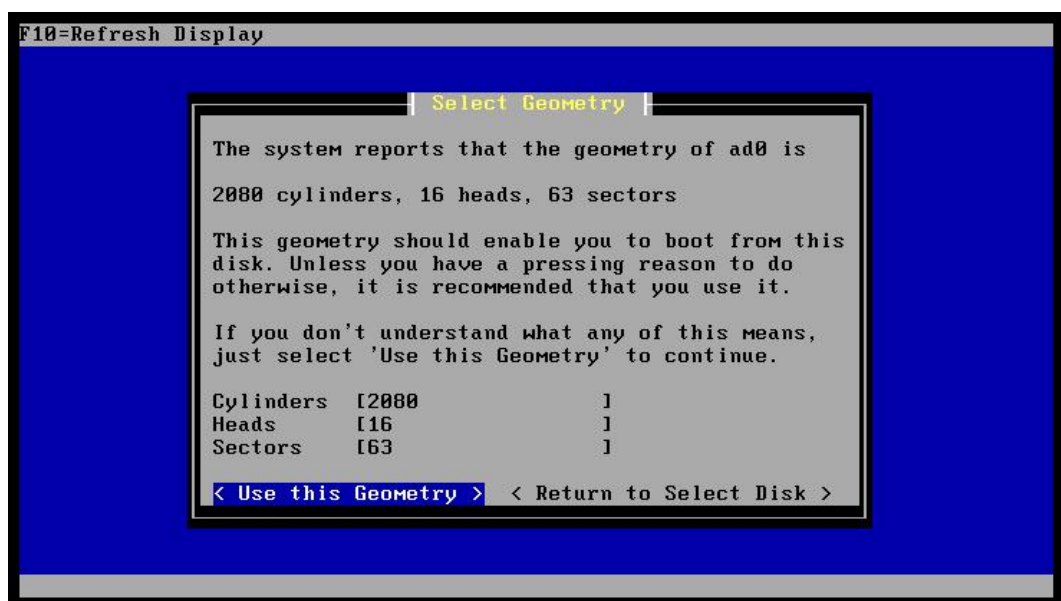


Figura 28: Confirmació dels paràmetres del disc.

En la Figura 5.11 ens mostra la geometria escollida per l'assistent. La que s'assigna per defecte ja ens va bé. Seleccionem "Use this Geometry".

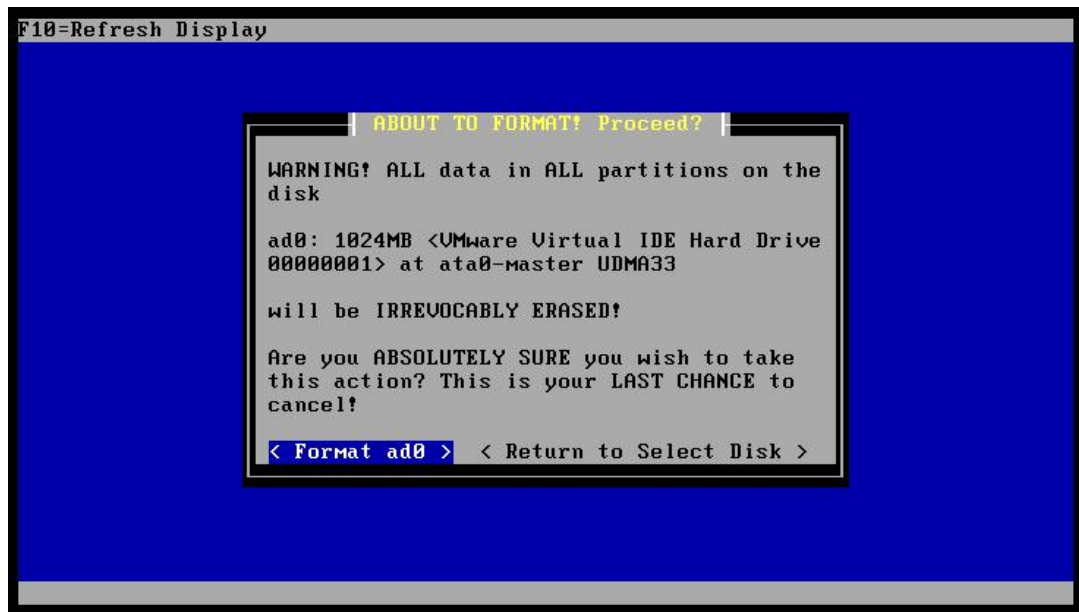


Figura 29: Confirmar la ordre de formatejar.

Un cop triades totes les configuracions anteriors és el moment de procedir amb la formatació del disc. Seleccionem "Format ad0".

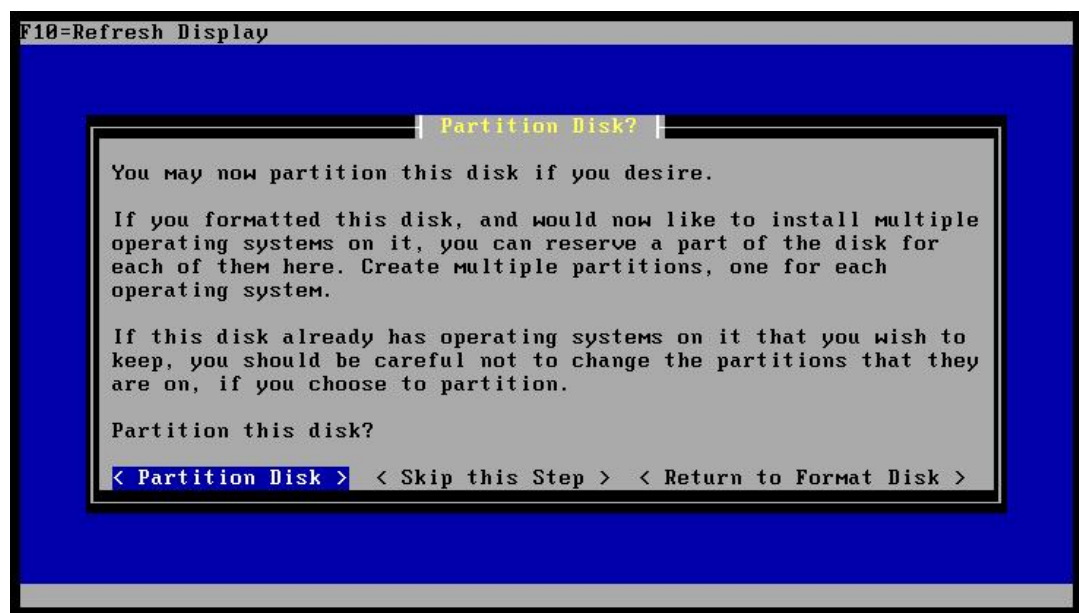


Figura 30: Particionament del disc.

En aquest moment ens dona l'opció de crear particions al disc. Seleccionem "Partition Disk".



Figura 31: Confirmació de les opcions de particionament.

L'assistent d'instal·lació ens escollirà una configuració recomanada que en el nostre cas ja ens va bé. Per tant seleccionem "Accept and Create".

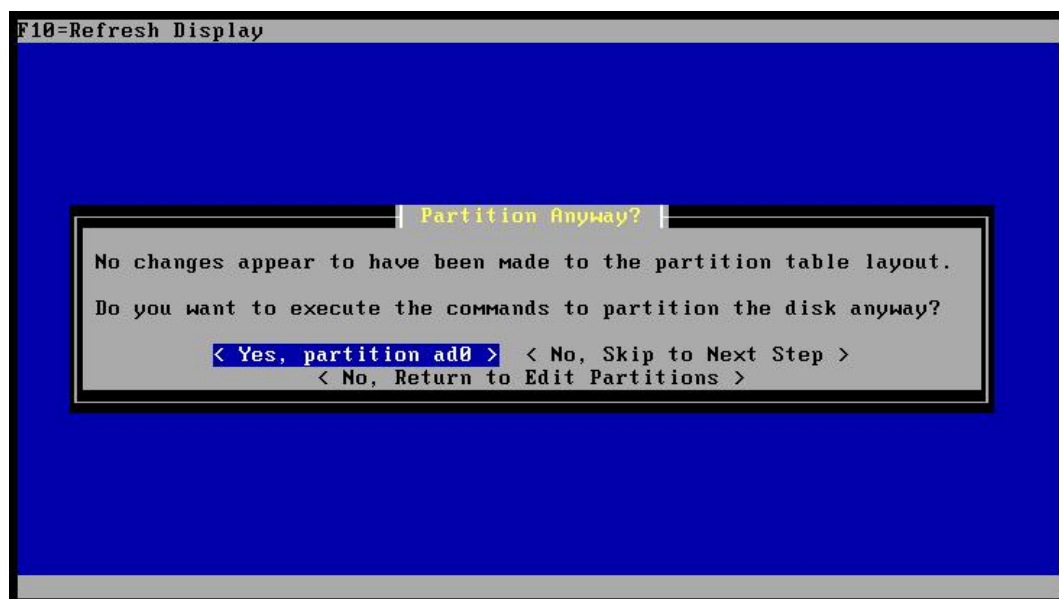


Figura 32: Confirmació del particionament.

En aquest punt confirmem els canvis escollits en apartats anteriors. Seleccionem "Yes, partition ad0".

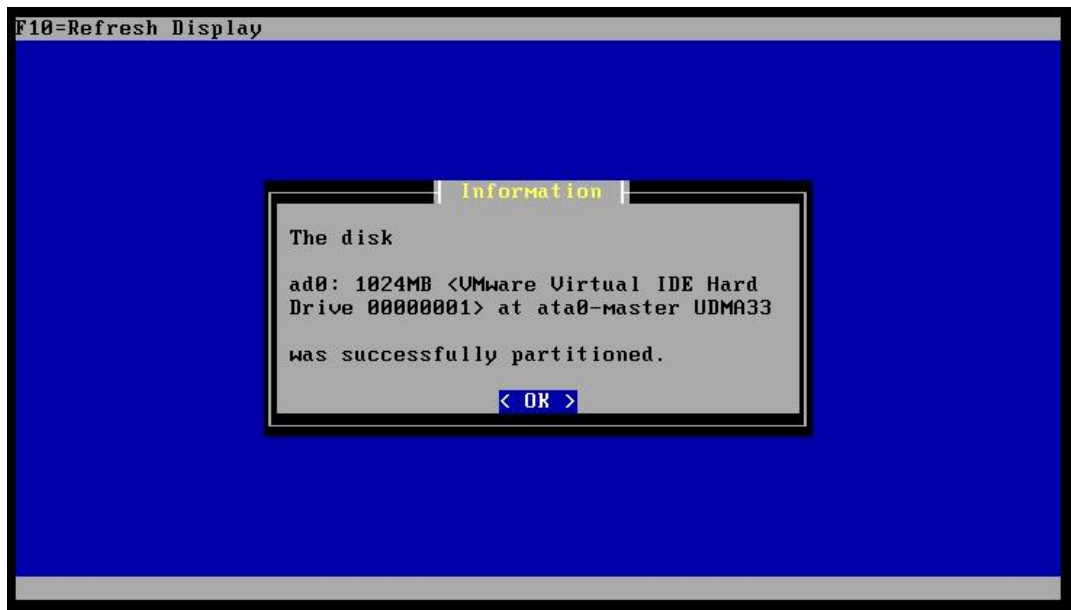


Figura 33: Formatació realitzada amb èxit.

Un cop particionat el disc, si tot ha anat bé ens apareixerà aquest missatge. Seleccionem "OK" per continuar.



Figura 34: Selecció de la partició formatada.

En aquesta figura seleccionem la partició on s'instal·larà el PfSense. En els passos anteriors ja ens hem assegurat de que el disc no te defectes, per tant, podem iniciar la instal·lació del PfSense.



Figura 35: Avís de que es perdràn les dades existents del disc.

Confirmem el inici de la instal·lació del PfSense seleccionant "OK". Ens avisa de que les dades emmagatzemades en el disc seran esborrades de forma irrevocable.



Figura 36: Partició formatada amb èxit.

Un cop eliminades les dades ens i formatat el disc ens haurà d'aparèixer aquest missatge confirmant que tot ha anat bé. Seleccionem "OK" per continuar.

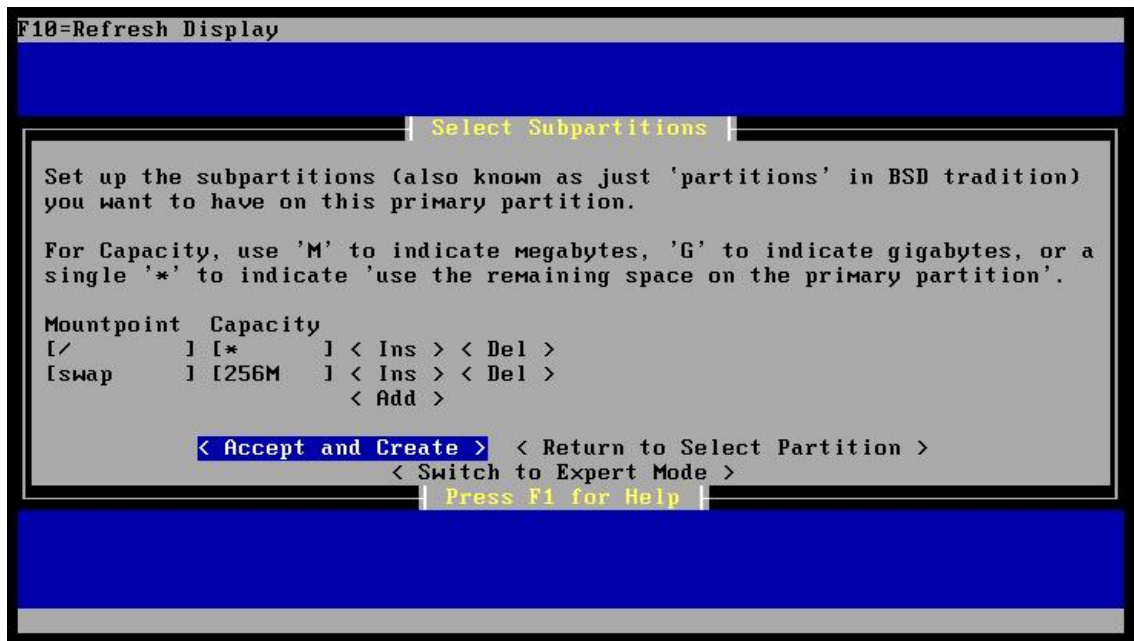


Figura 37: Confirmar les opcions de creació de les particions.

En aquesta figura es mostra tal com quedaran les particions del disc un cop instal·lat el sistema. S'assignen 256 MB per la partició d'intercanvi (SWAP) i la resta de la mida del disc s'assigna a la instal·lació del PfSense. Seleccionem "Accept and Create" per continuar.



Figura 38: Elecció del kernel que s'instal·larà.

En aquest punt l'assistent ens permet seleccionar el tipus de kernel a instal·lar. En el nostre cas seleccionem "Uniprocessor Kernel (one

processor)” ja que l’ordinador on instal·lem el PfSense només disposa d’un processador.

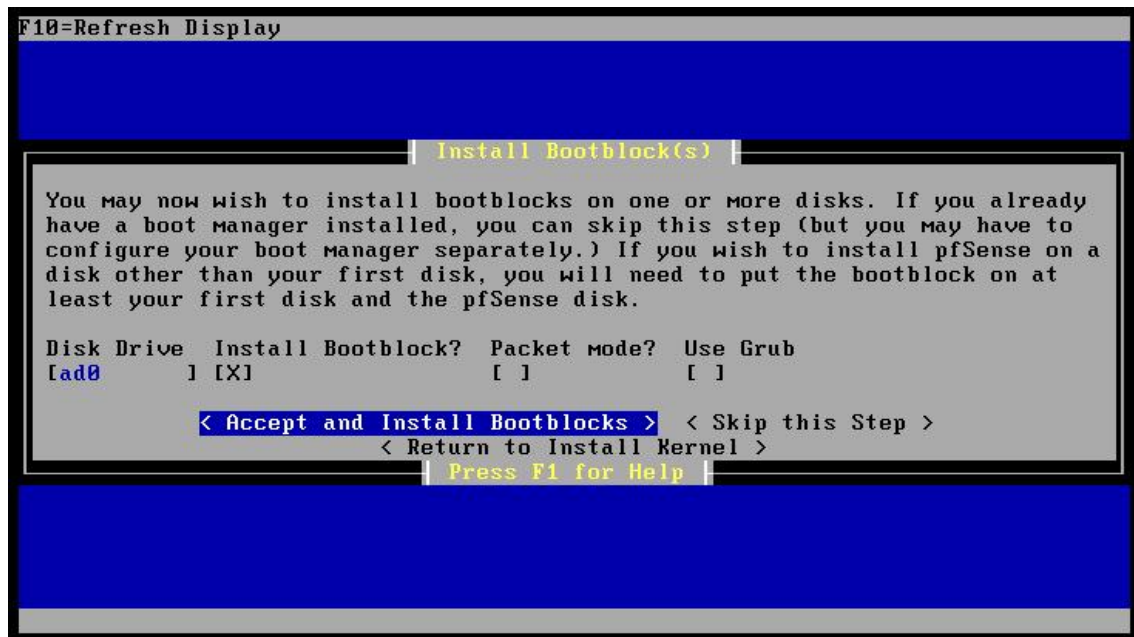


Figura 39: Instal·lació dels bootblocks.

En aquest punt de la instal·lació haurem de seleccionar on instal·lar els “Bootblocks” [18] (blocs d’arrencada). En el nostre cas volem que s’instal·lin en el mateix disc que utilitzem per la instal·lació del PfSense. Seleccionem “Accept and Install Bootblocks” per continuar.

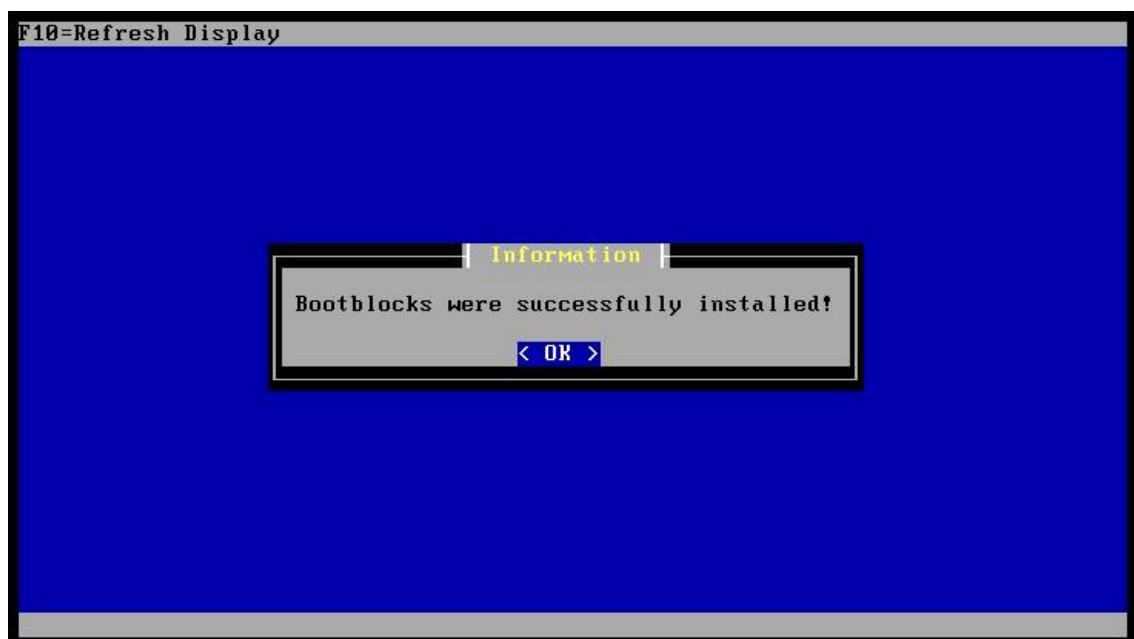


Figura 40: Èxit en la instal·lació dels Bootblocks.

En aquesta figura se'ns confirma la correcta instal·lació dels "Bootblocks". Seleccionem "OK".

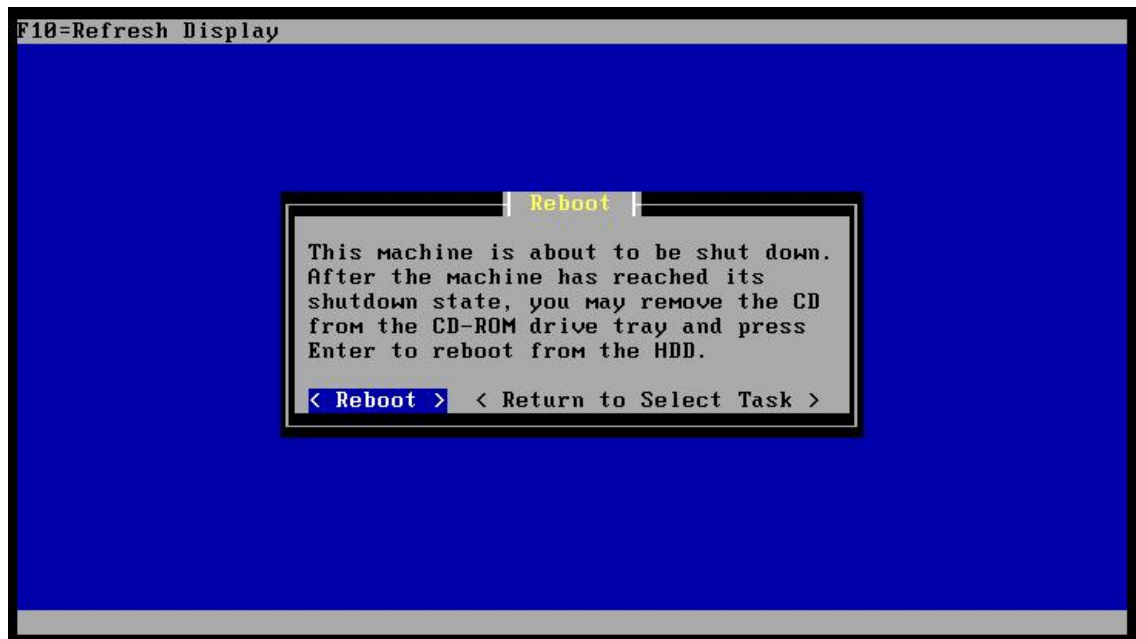


Figura 41: Reiniciar el sistema.

En aquest punt ja tenim el PfSense instal·lat al disc dur del nostre ordinador que actuarà com a Portal captiu. Reiniciem l'ordinador per a començar a utilitzar el PfSense. Traiem el cd-rom d'instal·lació i iniciem l'ordinador.

```
*** Welcome to pfSense 1.2-RELEASE-pfSense on pfSense ***

WAN*          ->  le0      ->  172.16.1.234(DHCP)
LAN*          ->  le1      ->  192.168.1.1

pfSense console setup
*****
0) Logout (SSH only)
1) Assign Interfaces
2) Set LAN IP address
3) Reset webConfigurator password
4) Reset to factory defaults
5) Reboot system
6) Halt system
7) Ping host
8) Shell
9) PFtop
10) Filter Logs
11) Restart webConfigurator
12) pfSense PHP shell
13) Upgrade from console

Enter an option: 2
```

Figura 42: Configuració de les interfícies de xarxa.

Un cop iniciat l'ordinador ens tornem a trobar amb la consola de configuració del PfSense. Es pot veure que ja no ens dona l'opció d'instal·lar el PfSense al disc dur del nostre ordinador. La configuració de les interfícies de xarxa s'ha establert automàticament. Per la interfície WAN s'ha assignat una adreça de la classe B (172.16.X.X/16). En el cas del centre s'assignarà una adreça de classe C (192.168.X.X/24), concretament: 192.168.0.12/24. Aquesta configuració s'escollirà des de la web d'administració del PfSense.

En aquest moment el que ens interessa és seleccionar l'adreça IP de la interfície LAN. Hem pres la decisió de crear la xarxa 192.168.3.0/24 per als usuaris que es connectin al portal captiu, d'aquesta manera separem les xarxes de dades de les que només volem donar accés a Internet. Escollim l'opció 2 i seguim els passos de la figura següent (Figura 5.26).

```
Enter an option: 2

Enter the new LAN IP address: 192.168.3.1

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new LAN subnet bit count: 24

Do you want to enable the DHCP server on LAN [y!n]? y
Enter the start address of the client address range: 192.168.3.100
Enter the end address of the client address range: 192.168.3.200
```

Figura 43: Establiment del rang de direccions del servidor DHCP.

A part de seleccionar la direcció IP, també activem el servidor DHCP que incorpora el PfSense per tal de facilitar l'assignació de direccions IP un cop connectats a la xarxa creada per la Interfície LAN. Per fer-ho seleccionem “y” i determinem el rang de direccions que assignarà el servidor DHCP.

```
Enter an option: 2

Enter the new LAN IP address: 192.168.3.1

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new LAN subnet bit count: 24

Do you want to enable the DHCP server on LAN [y!n]? y
Enter the start address of the client address range: 192.168.3.100
Enter the end address of the client address range: 192.168.3.200

The LAN IP address has been set to 192.168.3.1/24.
You can now access the webGUI by opening the following URL
in your web browser:

http://192.168.3.1/

Press ENTER to continue.


```

Figura 44: Confirmació de les opcions escollides.

Un cop tot instal·lat i establertes les configuracions IP de les interfícies de xarxa ja podem accedir a administrar el Pfsense mitjançant un navegador i accedint a la interfície LAN del PfSense. En el nostre cas introduïrem la direcció IP: **192.168.3.1**. Aquí ens demanarà les dades de

connexió, introduïrem les que venen per defecte que són: usuari: admin i password: pfsense.

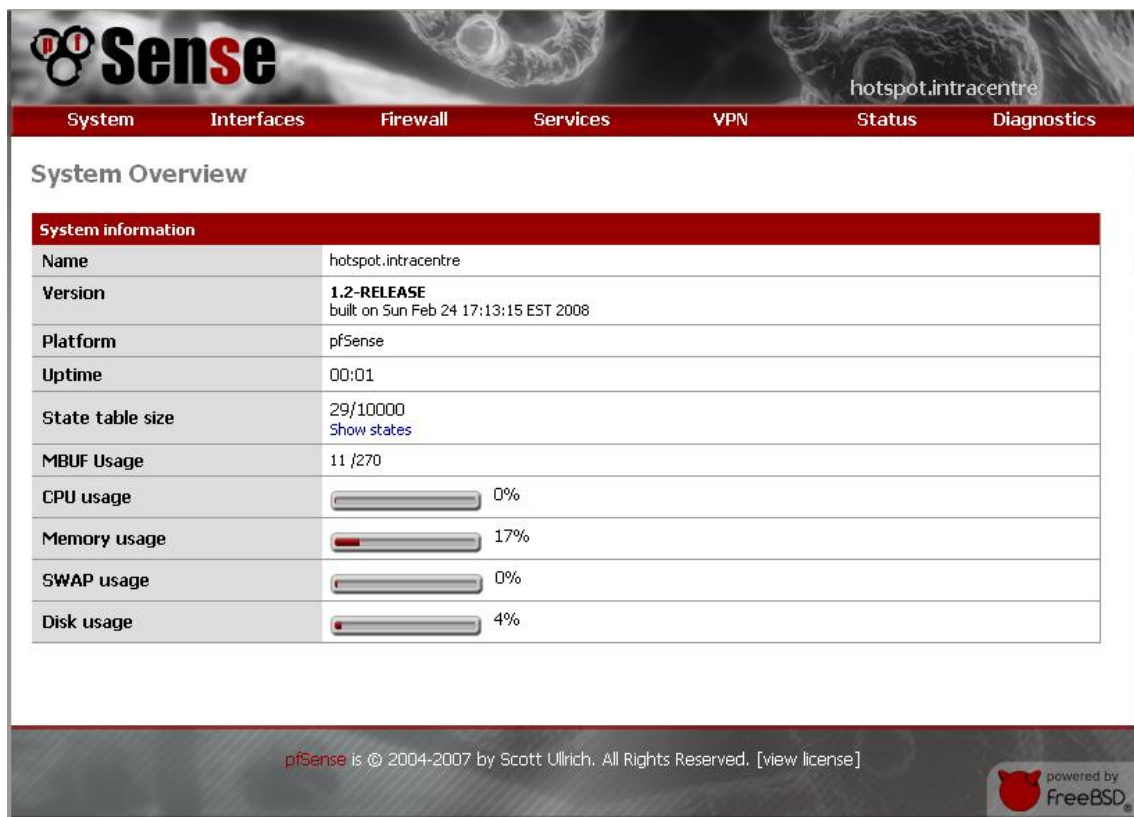


Figura 45: Pantalla inicial del PfSense.

La figura 5.28 ens mostra la pàgina inicial de configuració del PfSense. Per tal de continuar configurant el Portal captiu accedirem a la pestanya System, situada a la part superior esquerra i seleccionarem l'opció "General Setup".

System: General Setup

Hostname	hotspot <small>name of the firewall host, without domain part e.g. <i>firewall</i></small>
Domain	intracentre <small>e.g. <i>mycorp.com</i></small>
DNS servers	<div></div> <div></div> <small>IP addresses; these are also used for the DHCP service, DNS forwarder and for PPTP VPN clients</small> <input checked="" type="checkbox"/> Allow DNS server list to be overridden by DHCP/PPP on WAN <small>If this option is set, pfSense will use DNS servers assigned by a DHCP/PPP server on WAN for its own purposes (including the DNS forwarder). They will not be assigned to DHCP and PPTP VPN clients, though.</small>
Username	admin <small>If you want to change the username for accessing the webGUI, enter it here.</small>
Password	<div></div> (confirmation) <small>If you want to change the password for accessing the webGUI, enter it here twice.</small>
webGUI protocol	<input type="radio"/> HTTP <input checked="" type="radio"/> HTTPS
webGUI port	81 <small>Enter a custom port number for the webGUI above if you want to override the default (80 for HTTP, 443 for HTTPS). Changes will take effect immediately after save.</small>
Time zone	Etc/UTC <small>Select the location closest to you</small>
NTP time server	pool.ntp.org <small>Use a space to separate multiple hosts (only one required). Remember to set up at least one DNS server if you enter a host name here!</small>
Theme	nervecenter <small>This will change the look and feel of pfSense</small>

Figura 46: Configuració inicial del PfSense.

En aquesta Figura 5.29 podem veure la pàgina de configuració General del PfSense. En ella introduïrem el nom del ordinador (HotSpot) i el domini al que pertany (intracentre). També podem modificar el nom d'usuari per accedir a l'administració del PfSense i el password del mateix. En el nostre cas també habilitarem l'accés per HTTPS [20] al port 81 per tal d'accedir de forma segura al sistema. Per confirmar els canvis seleccionem "Save". Un cop aplicats ens canvis serem redireccionats de forma automàtica a la direcció: <https://192.168.3.1:81>. Per al protocol https el port per defecte és el 443 però nosaltres l'hem canviat pel 81 ja que no és un port que estigui documentat i per tant ens dona un punt més de seguretat.

The screenshot shows the PfSense configuration page for the WAN interface. The top navigation bar includes System, Interfaces, Firewall, Services, VPN, Status, and Diagnostics. The 'Interfaces: WAN' section is active. Under 'General configuration', the 'Type' is set to 'Static'. The 'MAC address' field is empty, with a 'Copy my MAC address' link and a note about spoofing. The 'MTU' field is also empty, with a detailed note about MSS clamping. Under 'Static IP configuration', the 'IP address' is '192.168.0.12' with a netmask of '24', and the 'Gateway' is '192.168.0.1'.

Figura 47: Establiment de la configuració de les interfícies de xarxa.

En la figura 5.30 hem establert la configuració que volem per la interfície WAN del PfSense. Per accedir a aquest apartat seleccionem la pestanya “Interfaces” seguit de l’opció “WAN”. La configuració que es veu en la figura serà l’escollida per nosaltres.

2. Configuració del Portal captiu per fer les validacions d’usuaris al PDC.

Un cop ja s’ha establert la configuració bàsica del Portal captiu, ara és el moment d’activar el servei del portal captiu i configurar-lo per tal de que els usuaris wi-fi siguin redireccionats a la pàgina de benvinguda. A més cal indicar en la configuració la direcció IP del ordinador que actua com a Servidor RADIUS (FreeRadius). En el nostre cas, haurem d’introduir la direcció IP que hem assignat a la segona interfície de xarxa del nostre servidor PDC. La direcció IP escollida és: 192.168.3.2. Aquesta direcció ha d’estar al mateix rang de xarxa que el PfSense per tal de que tots dos serveis es puguin passar les dades d’autenticació dels usuaris.

Per accedir a la configuració del Portal Captiu seleccionem la pestanya “Services” i després “Captive Portal”.

Services: Captive portal

Captive portal Pass-through MAC Allowed IP addresses Users File Manager

☒ **Enable captive portal**

Interface	LAN <input type="button" value="v"/> Choose which interface to run the captive portal on.
Maximum concurrent connections	<input type="text"/> per client IP address (0 = no limit) This setting limits the number of concurrent connections to the captive portal HTTP(S) server. This does not set how many users can be logged in to the captive portal, but rather how many users can load the portal page or authenticate at the same time! Default is 4 connections per client IP address, with a total maximum of 16 connections.
Idle timeout	60 <input type="text"/> minutes Clients will be disconnected after this amount of inactivity. They may log in again immediately, though. Leave this field blank for no idle timeout.
Hard timeout	<input type="text"/> minutes Clients will be disconnected after this amount of time, regardless of activity. They may log in again immediately, though. Leave this field blank for no hard timeout (not recommended unless an idle timeout is set).
Logout popup window	<input checked="" type="checkbox"/> Enable logout popup window If enabled, a popup window will appear when clients are allowed through the captive portal. This allows clients to explicitly disconnect themselves before the idle or hard timeout occurs.
Redirection URL	http://www.iesborrevicens.cat If you provide a URL here, clients will be redirected to that URL instead of the one they initially tried to access after they've authenticated.
Concurrent user logins	<input type="checkbox"/> Disable concurrent logins If this option is set, only the most recent login per username will be active. Subsequent logins will cause machines previously logged in with the same username to be disconnected.
MAC filtering	<input type="checkbox"/> Disable MAC filtering If this option is set, no attempts will be made to ensure that the MAC address of clients stays the same while they're logged in. This is required when the MAC address of the client cannot be determined (usually because there are routers between pSense and the clients). If this is enabled, RADIUS MAC authentication cannot be used.
Authentication	<input type="radio"/> No authentication <input type="radio"/> Local user manager <input checked="" type="radio"/> RADIUS authentication Primary RADIUS server IP address <input type="text" value="192.168.3.2"/> Enter the IP address of the RADIUS server which users of the captive portal have to authenticate against.

Figura 48: Configuració del Portal Captiu.

En la figura 5.30 podem veure com hem de configurar el Portal Captiu per tal de que faci les validacions contra el servidor d'autenticació RADIUS instal·lat en el nostre PDC. Primerament hem de dir-li quina interfície rebrà les peticions de validació dels usuaris wi-fi, en el nostre cas serà la Interfície LAN. En segon lloc hem establert que el temps màxim que els clients podran estar connectats serà 60 minuts, passat aquest temps hauran de tornar a introduir les dades de connexió per poder estar connectats a la xarxa. També habilitem l'opció d'activar una finestra emergent (pop-up) que permeti als usuaris desconnectar-se del sistema de forma voluntària. El Portal Captiu també ens permet introduir la direcció web on els usuaris seran redireccionats un cop s'hagin validat al sistema, en el nostre cas serà la plana web del Institut. El proper pas és introduir en quina direcció IP de la xarxa hi ha instal·lat el servidor RADIUS i el password que s'intercanviaran els dos serveis per a fer les

autenticacions dels usuaris. En el nostre cas només tenim un servidor RADIUS, el que farem és repetir la configuració en la configuració del servidor RADIUS secundari. Veieu Figura 5.31.

Com a alternativa a servidor RADIUS podem utilitzar el de la plataforma XTEC. D'aquesta forma, el personal docent extern al centre en qüestió també podria fer ús de la xarxa wi-fi del centre i no hauria de recórrer al coordinador d'informàtica per a que li facilités les dades de configuració de la xarxa sense fils.

Dades de connexió del servidor RADIUS de XTEC:

IP dels servidor de RADIUS: 213.176.161.14

Port: 1814

Contrasenya: wificentres

The screenshot shows the 'Authentication' tab in PfSense. Three radio buttons are visible: 'No authentication' (unselected), 'Local user manager' (unselected), and 'RADIUS authentication' (selected). Below this, the 'Primary RADIUS server' section contains three input fields: 'IP address' (192.168.3.2), 'Port' (blank), and 'Shared secret' (passwordportal). A secondary section for 'Secondary RADIUS server' also contains three input fields: 'IP address' (192.168.3.2), 'Port' (blank), and 'Shared secret' (passwordportal). Each input field has a small text box below it providing instructions or default values.

Authentication	
<input type="radio"/> No authentication	
<input type="radio"/> Local user manager	
<input checked="" type="radio"/> RADIUS authentication	
Primary RADIUS server	
IP address	192.168.3.2 <small>Enter the IP address of the RADIUS server which users of the captive portal have to authenticate against.</small>
Port	 <small>Leave this field blank to use the default port (1812).</small>
Shared secret	passwordportal <small>Leave this field blank to not use a RADIUS shared secret (not recommended).</small>
Secondary RADIUS server	
IP address	192.168.3.2 <small>If you have a second RADIUS server, you can activate it by entering its IP address here.</small>
Port	 <small>Leave this field blank to use the default port (1812).</small>
Shared secret	passwordportal <small>Leave this field blank to not use a RADIUS shared secret (not recommended).</small>

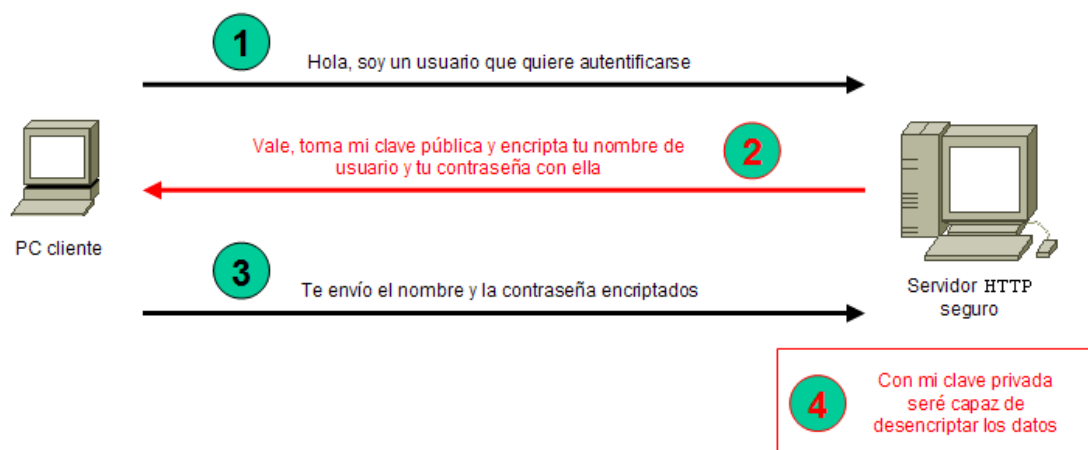
Figura 49: Configuració de l'apartat RADIUS del PfSense.

Detall de configuració del Portal Captiu.

[illegible]

Figura 50: Configuració del Servidor HTTPS.

Per tal de garantir la seguretat de les dades que els usuaris han d'introduir en el procés de validació habilitem l'opció "Enable HTTPS login". En aquest punt introduïrem el nom de l'ordinador on s'ha generat el certificat, així com el certificat i la clau privada. Podem crear el certificat des del mateix software PfSense. Per fer-ho anem a la pestanya "System" i l'opció "Advanced". Trobarem l'opció "create" i facilitarem les dades que se'ns demanen. Un cop generat el certificat l'introduïrem en l'apartat de configuració del Portal Captiu.



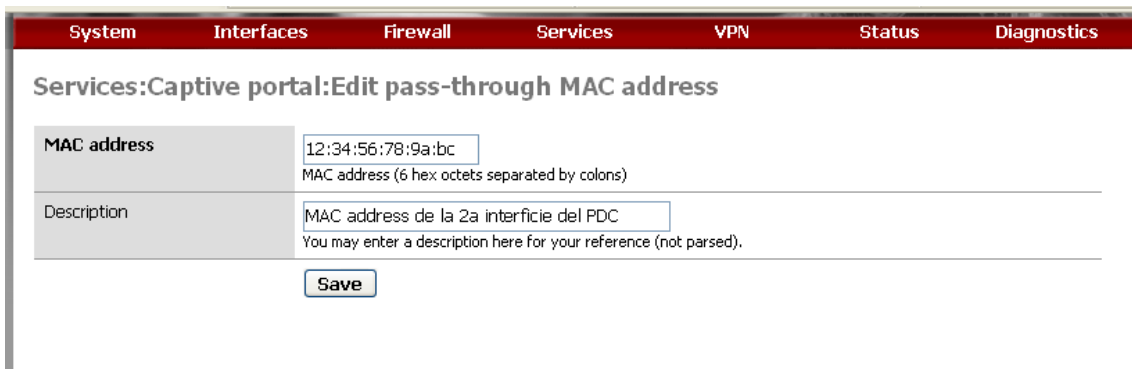
Fundamentos de la autenticación segura

Figura 51: Esquema de funcionament del protocol HTTPS.

PfSense també ens dona l'opció de modificar el disseny de la pàgina web que es mostrarà als usuaris un cop vulguin accedir a la xarxa, així

com també la pàgina web d'error que es generaria en cas de que les dades no siguin correctes. Aquesta plana ha de contenir uns camps específics per tal de que el procés de validació i re direcció dels usuaris funcioni correctament.

L'altre apartat important que cal configurar és el de: "Pass-through MAC". El Pass-through MAC ens serveix per donar d'alta la direcció física [21] (MAC Address) de les interfícies de xarxa que no han de passar pel procés d'autenticació. En el nostre cas hem d'introduir la MAC Address de la segona tarja de xarxa del servidor (amb IP 192.168.3.2), ja que si no ho féssim, el Portal Captiu i el PDC no s'intercanviarien les dades d'autenticació dels usuaris perquè el Pfsense no deixaria rebre cap resposta des del PDC, ja que aquest últim no hauria passat pel procés d'autenticació. En aquest apartat hauríem de donar d'alta a tots els dispositius o equips que no volem que passin pel procés de validació. En el nostre cas només ens cal donar d'alta el Servidor PDC.



The screenshot shows the PfSense web interface. The top navigation bar has tabs for System, Interfaces, Firewall, Services, VPN, Status, and Diagnostics. The 'Services' tab is selected, and the sub-tab 'Captive portal' is active. The main heading is 'Services:Captive portal:Edit pass-through MAC address'. Below this, there is a form with two main sections: 'MAC address' and 'Description'. The 'MAC address' section has a text input field containing '12:34:56:78:9a:bc' and a label 'MAC address (6 hex octets separated by colons)'. The 'Description' section has a text input field containing 'MAC address de la 2a interfície del PDC' and a label 'You may enter a description here for your reference (not parsed)'. At the bottom of the form is a 'Save' button.

Figura 52: Configuració del Pass-through.

El funcionament del procés de validació dels usuaris és molt senzill. Un usuari de la xarxa es connecta al punt d'accés inal·làmbic, i mitjançant el servidor DHCP del PfSense rebra la configuració IP per a poder accedir a Internet. Un cop que l'usuari obre el navegador web es mostra la pàgina de benvinguda del Portal Captiu. En ella haurà d'introduir les dades de validació que se li ha facilitat i acceptar. En aquest moment es posa en marxa el procés de validació de l'usuari. El PfSense envia una petició d'accés (Access-request) al Servidor RADIUS, aquest comprova a la seva base de dades LDAP si l'usuari existeix. En cas afirmatiu el PfSense rebra del Servidor RADIUS el "Access-Accept" i permet a l'usuari l'accés a Internet redireccionant a l'usuari a la pàgina web definida en la configuració (també s'habilita el pop-up de logout per l'usuari). En cas contrari el PfSense rebra el "Access-Reject" i es mostrarà la pàgina d'error a l'usuari.

Backup de la configuració del PfSense:

En aquest moment ja podem començar a utilitzar el portal captiu validant-nos en ell introduint les dades facilitades.

Ara és el moment de realitzar una còpia de seguretat (Backup) de les configuracions introduïdes fins al moment. D'aquesta forma, si en algun moment ens fa falta restablir la configuració ho podrem fer de forma còmoda i ràpida.

Per tal de fer el Backup obrirem el navegador web, ens validarem en la pàgina de benvinguda del portal captiu i entrarem a la direcció: <https://192.168.3.1:81> i ens validem com usuaris administradors. Usuari: admin i contrasenya: pfsense (si no les hem canviat, ja que són les que venen per defecte).

Accedim a l'opció "Diagnostics" i seleccionem l'opció "Backup/Restore". En apareixerà la següent pantalla.

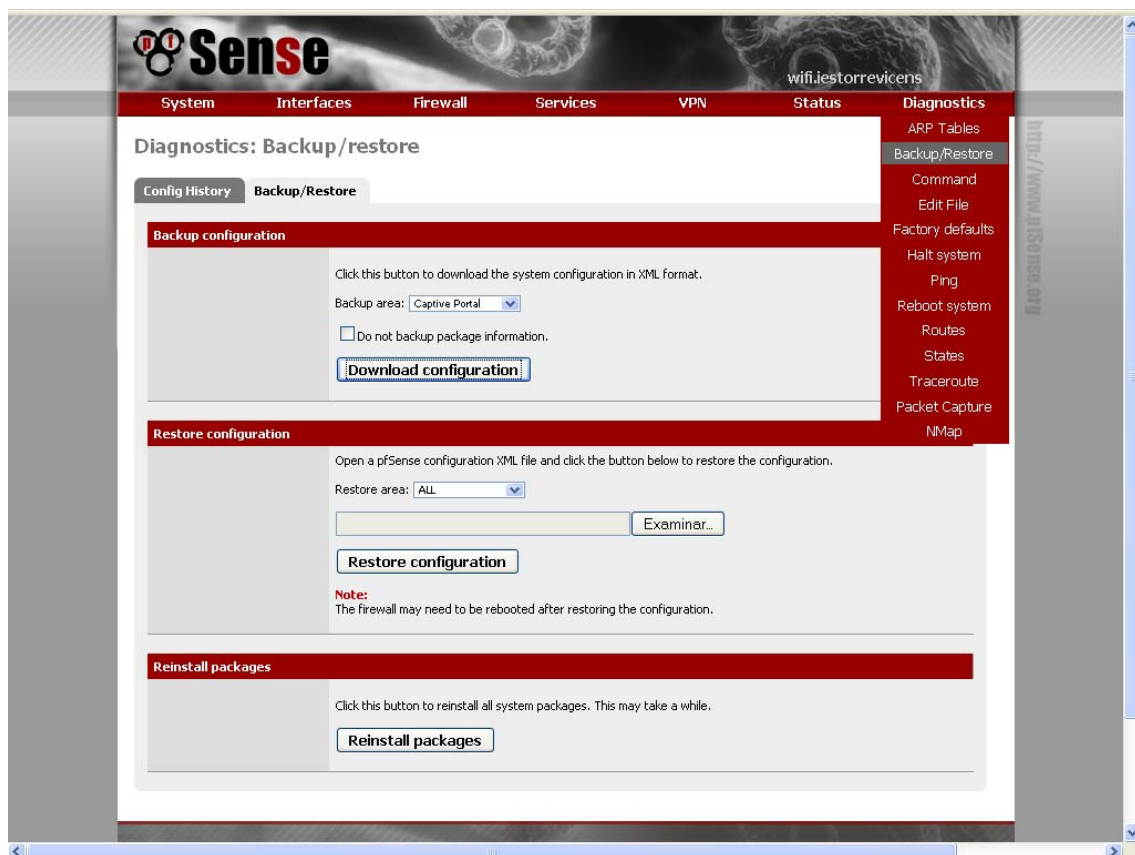


Figura 53: Pantalla de Back Up del Pfsense.

Es pot veure en l'apartat de Backup que podem realitzar un Backup personalitzat de cada servei del PfSense o de la configuració global. En el nostre cas farem un Backup de tot el sistema. Fem clic sobre l'opció: "Download configuration". Això ens exportarà un fitxer .xml [22] amb tota la configuració. Aquest fitxer serà el que ens serviria en cas de fallida per a restablir els serveis del Pfsense (és recomanable guardar-lo fora del servidor).

Per fer la restauració anirem a l'apartat de restauració ("Restore configuration"), fem clic sobre l'opció "Examinar..." i seleccionem el fitxer de Backup. El PfSense es reiniciarà amb les configuracions restablertes.

3. Punts d'accés sense fils.

Fins al moment hem establert totes les configuracions per ficar en funcionament tots els serveis que volem oferir. Totes aquestes configuracions només ens permetran accedir a la xarxa als usuaris que ens connectem a la xarxa creada per el Pfsense. El que ens interessa és accedir a aquest servei de forma inal·làmbrica.

Per tal de fer-ho possible necessitarem ficar en funcionament el punts d'accés inal·làmbric (Access Point). Aquests dispositius transformen la senyal cablejada amb inal·làmbrica, per tant, realitzen la funció que ens interessa.

En el nostre cas posarem en funcionament tants punt d'accés com necessitem per a cobrir l'àrea on volem donar aquest servei wi-fi. S'intentarà establir l'efecte "*roaming*" (itinerància), de forma que un dispositiu es podrà moure per tota la zona de cobertura i registrant-se als diferents dispositius wi-fi (Access Point). Per a que aquest efecte sigui possible, haurà d'haver una superposició (overlapping) en les cobertures dels diferents punts d'accés, del tal manera que els usuaris es puguin moure pel centre i sempre tinguin cobertura. Tots els punt d'accés s'hauran de configurar per a que puguin funcionar dins del rang de xarxa creat per el PfSense, per tant, a la xarxa 192.168.3.0/24.

En aquest moment, dins la xarxa 192.168.3.0/24 ja hi tenim funcionant 2 dispositius, el PDC i el Pfsense. Aquest últim el tenim configurat per a que doni direccions IP automàticament (DHCP) a partir de la direcció 192.168.3.100 fins 192.168.3.200. Per tant encara podem donar direccions des de 192.168.3.3 fins 192.168.3.99 i des de 192.168.201 fins 192.168.3.254. Per ara, creiem que amb 100 direccions ja podem donar servei al % d'usuaris que utilitza el sistema simultàniament fins al

moment. En cas que el nombre d'usuaris augmentes molt podríem augmentar el rang de direccions establert pel servidor DHCP, crear una altra xarxa d'accés wi-fi o fins i tot modificar el rang de direccions, és a dir, passar del rang de direccionament de Classe C (actual) al de Classe B.

En el nostre cas començarem a configurar els punt d'accés a partir de la direcció 192.168.3.10. De forma que un AP (Access Point) haurà de tenir els següents paràmetres de configuració.

Direcció IP: 192.168.3.10
Mascara de xarxa: 255.255.255.0
Porta d'enllaç: 192.168.3.1

Les direccions dels Servidors DNS ja les establirà el PfSense mitjançant el servidor DHCP. Nosaltres només hem d'establir la configuració necessària per que els AP i el PfSense es puguin comunicar.

Connexió a la xarxa sense fils:

Connectem la tarja inal·làmbrica del nostre dispositiu i busquem la senyal wi-fi: **wifi_torre_vicens**. Al connectar-nos el servidor DHCP del Pfsense ens assignarà les configuracions de xarxa automàticament.

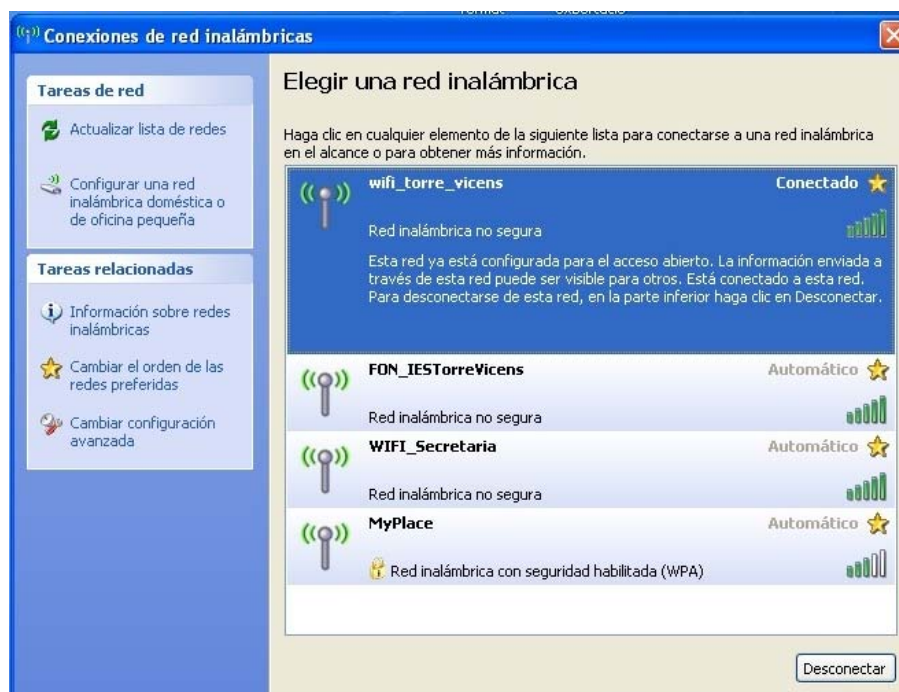


Figura 54: Detecció de les xarxes sense fils.

Al obrir el navegador, enlloc de carregar-se la pàgina web que tenim configurada com a pàgina d'inici, ens apareixerà la pàgina del portal captiu següent:



Benvingut a la wifi de l'IES Torre Vicens

Introdueix el teu nom d'usuari i contrasenya per accedir a internet.

Username:

Password:

Figura 55: Pàgina web de benvinguda del Portal Captiu.

Introduïrem les dades de connexió i ja tindrem accés a Internet. En cas de que les dades de connexió hagin estat introduïdes de forma errònia, ens apareixerà la següent plana web:

Error d'autenticació.

Nom d'usuari i/o contrasenya invàlids.

[Ves enrere](#) per tornar-ho a provar.

Figura 56: Pàgina d'error d'autenticació.

Missatge d'error, les dades introduïdes no són vàlides.



Figura 57: Pàgina web on serem redireccionats i finestra emergent de desconnexió.

Si les dades de validació introduïdes eren correctes, serem redireccionats a la plana web del centre.

Capítol 6: Creació del Live CD.

1. *Guia de creació del Live CD.*

“Un Live cd o Live DVD, genèricament LiveDistro, (traduït de vegades com CD Viu o CD autònom), és un sistema operatiu (normalment acompanyat d'un conjunt d'aplicacions) emmagatzemat en un mitjà extraïble, tradicionalment un CD o un DVD (d'aquí els seus noms), que pot executar-se des del mateix sense necessitat d'instal·lar-lo en un disc dur d'un ordinador, per la qual cosa utilitza la memòria RAM com a disc dur virtual i el propi mitjà com a sistema de fitxers.”

En el nostre treball volem crear un Live CD que contingui tots els paquets (programes) necessaris per a la posada en funcionament del nostre servidor.

La creació del Live CD es realitzarà des del Servidor que hem instal·lat de forma manual i que ens ha servit per a realitzar les proves necessàries. En el servidor es pot instal·lar el programari necessari per a crear el Live CD i a més ja tenim els serveis ben configurats.

El programari necessari per a la creació del Live CD no està inclòs dins dels repositoris actuals ja que estem utilitzant la versió estable de Debian (Etch) [24], per tant, haurem de modificar els repositoris i actualitzar la llista de paquets disponibles.

Per fer això fem des de la consola:

```
#vi m /etc/apt/sources. l i st
```

I afegim al final la següent línia:

```
deb http://www.backports.org/debian etch-backports  
mai n contri b non-free
```

guardem el fitxer amb: Ctrl+C i :wq + Enter

Actualitzem la llista de paquets amb:

```
# apt-get update
```

Per poder utilitzar aquests repositoris hem d'instal·lar el següent:

```
#apt-get install debian-backports-keyring
```

Actualitzem la llista de paquets amb:

```
# apt-get update
```

Ara ja ho tenim tot preparat per a instal·lar el programari necessari per la creació del Live CD. El paquet de Debian que ens ajudarà a crear el Live CD és el “live-helper”. Anem a instal·lar-lo:

```
#apt-get install live-helper
```

2. Opcions en la creació d'un Live CD.

A l'hora de crear un Live CD disposem d'un ampli ventall de possibilitats de configuració que ens permeten crear un “cd viu” que s'ajusti al màxim a les nostres necessitats i configuracions.

En el nostre cas necessitem crear un Live CD molt ben definit i que a part d'incloure la instal·lació dels serveis necessaris, també disposi dels fitxers de configuració d'aquests serveis. Amb això aconseguirem crear una eina que ens permetrà ficar en funcionament un sistema complex amb un temps molt ajustat.

Tots aquest ajustaments es realitzen mitjançant l'execució de l'ordre:

```
#lh_config
```

Després d'aquesta instrucció s'enumeren tots els parametres necessaris per crear el nostre Live CD. En el nostre cas la instrucció que ens ha permès crear el nostre “cd viu” és:

```
# lh_config -a i386 -d etch --hostname pdc --
bootappend "locale=es_ES.UTF-8 keyb=es" -p xfce-
desktop --packages "openssh-server make gcc gcc++
gengetopt libpopt-dev python-crypto slapd ldap-utils
apache-ssl smbldap-tools phpLDAPadmin samba samba-doc
libnss-ldap libpam-ldap nscd freeradius freeradius-
ldap rsync open-ssl libnet-ssleay-perl libauthen-pam-
perl libio-pty-perl libmd5-perl" && lh_build
```

Anem a detallar i explicar cadascun dels paràmetres introduïts.

Opció: -a i386

Especifica l'arquitectura del microprocessador on "viura" el nostre Live CD. Si vulguessim fer servir el Live CD sota una arquitectura de processador AMD de 64 bits (AMD64) caldria especificar l'opció:

-a amd64

Opció: -d etch

Aquesta opció especifica la distribució de Debian que volem utilitzar per crear el Live CD. En el nostre cas es la Distribució Etch (última versió estable d'aquest sistema operatiu). També podríem utilitzar altres distribucions o version com lenny (testing, està en fase de proves) o sid (inestable, la que es troba en fase de desenvolupament).

Opció: --hostname pdc

Ens permet especificar el nom de màquina (nom del host) que tindrà el nostre Live CD un cop iniciat.

Opció: --bootappend "locale=es_ES.UTF-8 keyb=es"

Amb aquest parametre aconseguim crear un Live CD amb l'idioma espanyol i el teclat també espanyol. Si no s'indica aquest parametre s'assignarà l'idioma i el teclat anglès.

Opció: -p xfce-desktop

Aquest paràmetre ens ha permès escollir l'entorn gràfic que utilitzarem en el nostre Live CD. Nosaltres hem escollit l'entorn XFCE, ja que és el més lleuger de tots els entorns gràfics existents.

Opció: --packages "openssh-server make gcc gcc++ gengetopt libpopt-dev python-crypto slapd ldap-utils apache-ssl smbldap-tools phpldapadmin samba samba-doc libnss-ldap libpam-ldap nscd freeradius freeradius-ldap rsync open-ssl libnet-ssleay-perl libauthen-pam-perl libio-pty-perl libmd5-perl"

Aquesta opció es una de les més importants, ja que ens permet agregar tots els paquets necessaris per poder ficar en funcionament els serveis implantats en el nostre PDC, si us fixeu, son els mateixos que hem instal·lat manualment al Capítol 4.

Opció: && lh_build

Amb aquesta última opció fem possible la creació de la imatge ISO que després gravarem en un cd-rom. Aquesta opció recull tots els parametres de "lh_config" i els integra tots en una fitxer (imatge ISO).

3. *Instal·lació del Live CD.*

En aquest treball de final de carrera s'ha creat un Live CD que facilita la posada en funcionament d'un PDC. Amb això aconseguim reduir la complexitat de la instal·lació d'aquest servidor.

Un cop realitzat aquest Live CD va sorgir la idea de poder instal·lar aquest "cd viu" al disc dur de l'ordinador que havia d'actuar com a PDC. Aquesta opció ens permetria utilitzar un disc dur de gran capacitat per allotjar les dades dels usuaris i per tant poder realitzar canvis de forma persistent.

En el fet d'aconseguir aquest propòsit ens trobem amb una sèrie de limitacions que ens impedeixen portar a terme aquesta idea. Aquests inconvenients són que el programari de Debian que ens permetria assolir el nostre objectiu encara es troba en fase de prova. En un principi no sembla que això sigui realment un problema, però si ens parem a pensar amb les premisses bàsiques que hem seguit durant l'elaboració d'aquest projecte veiem que no podem portar a terme aquesta idea, ja que el fet d'oferir aquesta funcionalitat ens "desmuntaria" la idea sobre la qual s'ha basat aquest projecte, estabilitat i utilització de programari estable que ens eviti problemes indesitjats.

No volem deixar a l'aire la forma en que s'afegiria aquesta funcionalitat, ja que un cop aparegui la versió estable del programari necessari, ja ens serà possible portar a terme el nostre propòsit.

El programari de Debian que ens permet realitzar la instal·lació d'un Live CD a un ordinador és: "live-installer". En el nostre cas el que hauriem de fer és afegir aquest paquet a la llista de paquets que hem utilitzar durant la creació del Live CD.

Per tant, i basant-nos amb les explicacions donades en l'apartat 2 d'aquest capítol, hauriem d'afegir el nom d'aquest paquet en la següent ordre:

```
# lh_config -a i386 -d etch --hostname pdc --
bootappend "local e=es_ES.UTF-8 keyb=es" -p xfce-
desktop --packages "openssh-server make gcc gcc++
gengetopt libpopt-dev python-crypto slapd ldap-utils
apache-ssl smbldap-tools phpLDAPadmin samba samba-doc
libnss-ldap libpam-ldap nscd freeradius freeradius-
ldap rsync open-ssl libnet-ssleay-perl libauthen-pam-
perl libio-pty-perl libmd5-perl live-installer" &&
lh_bulld
```

Un cop generat, grabat en un cd-rom la imatge ISO, i arrencat el Live CD, ens trobariem en disposició d'instal·lar el nostre Live CD al disc dur de l'ordinador que actuarà com a PDC.

Per tenir més informació sobre el paquet "live-installer" segueix aquest enllaç:

[Debian-installer's component for installing \(copying\) LiveCD to hard disk](https://launchpad.net/live-installer)

<https://launchpad.net/live-installer>

4. Importació de la configuració del PDC.

Un cop ja hem creat el nostre Live CD amb el programari necessari, anem a explicar com realitzariem la importació dels fitxers de configuració que hem extret del nostre PDC de proves.

Tal i com hem explicat a l'apartat 5 del capítol 4 (vegeu pàg. 44), podem importar i exportar els fitxers de configuració del nostre PDC de proves. En el nostre cas el que necessitem és primerament exportar els fitxers de configuració que hem personalitzat en el nostre servidor PDC de proves, i després importar aquests fitxers al Servidor PDC que hem carregat des del Live CD creat.

Amb aquesta acció tindrem al nostre servidor (Live CD) els fitxers de configuració que ens permetran tenir ben configurats els serveis que volem implantar. Després d'això, només ens caldrà reiniciar els serveis mitjançant:

```
#/etc/init.d/nom_del_servei restart
```

i *en teoria* ja tindrem funcionant el nostre servidor PDC des del Live CD que hem creat.

L'altra forma de realitzar aquesta importació de fitxers és incloure els fitxers de configuració durant el procés de creació del Live CD. És a dir, mitjançant els paràmetres de configuració que ens ofereix el servei "live-helper", incloure els fitxers dins la imatge ISO que generem durant el procés de creació del Live CD.

Amb això aconseguim generar un "cd viu" amb les configuracions ja establertes, la qual cosa ens permet realitzar la implantació del Servidor PDC d'una forma més fàcil i ràpida.

A priori tot sembla indicar que el nostre Live CD compleix tots els objectius que ens hem marcat des d'un principi, però malauradament, no acaba funcionant com ens esperavem.

Quan hem realitzat les proves amb el Live CD ens hem trobat amb una sèrie de problemes que fan que el "cd viu" creat no actuï com desitgem. Anem a detallar els problemes que tenim.

Per una banda, si creem el Live CD incloent els fitxers de configuració durant el procés de creació de la imatge ISO ens trobem amb el problema de que no podem validar-nos com usuaris del sistema un cop arribem a la pantalla de validació. Hem probat de validar-nos amb l'usuari que es crea per defecte "user" i contrasenya "live" i també s'ha probat de tornar a crear el Live CD indicant el nom d'usuari que volem que es creï com a usuari per defecte del nostre Live CD. Aquests dos intents de solució no ens han servit i per tant s'han acabat desestimant.

Per altra banda, si generem el Live CD sense incloure els fitxers de configuració, i arranquem el Live CD, aquest cop es realitza el procés de login automàticament, és a dir, generem un "cd viu" amb l'opció de "autologin" per defecte. A priori aquesta opció ja ens ha anat bé, ja que podem arribar més lluny que en l'altre cas. És a dir, en aquest cas podem assignar un password a l'usuari "root" mitjançant:

#sudo passwd

i establint el password que volem per l'usuari "root", per exemple, "password".

També podem afegir l'usuari "admin", ja que aquest és el nom d'usuari que necessitem per administrar el servei LDAP mitjançant el PHPLDAPADMIN. Ho fem amb:

#useradd admin

I assignem un password amb:

#passwd admin

Fins aquí tot va bé, la sorpresa ens la trobem quan intentem validar-nos al PhpLdapAdmin, ja que, no aconseguim entrar i per tant no podem començar amb la importació i tractament dels usuaris.

S'ha intentat reconfigurar tots els serveis seguint els passos esmentats al capítol 4, i s'han repassat totes les configuracions del fitxers per assegurar-nos de que no sigui un problema de configuracions. A totes aquestes revisions no hi hem trobat res que ens solucioni el problema. A priori pot donar la sensació de que no hem creat bé l'usuari "admin",

però el dubte es dilueix quan intentem accedir al Servidor PDC (Live CD) mitjançant una sessió SSH.

Utilitzant el client ssh "Putty", indicant la direcció IP del Servidor PDC, el nom d'usuari "admin" i el password, podem entrar al sistema com a usuari "admin", la qual cosa significa que hem creat l'usuari "admin" correctament.

Fins al moment no s'ha trobat una solució a aquest problema, per la qual cosa, deixem la resolució d'aquest conflicte com a aspectes a millorar en treballs futurs.

Capítol 7: Inserció dades d'usuari al sistema.

1. Exportació de dades de SAGA.

En aquest primer apartat del capítol 7 explicarem com realitzar la exportació de les dades dels usuaris des de la plataforma "SAGA" (Sistema d'Administració i Gestió Acadèmica) del Departament d'Educació de la Generalitat de Catalunya. SAGA és un programa en entorn web que ha esdevingut una eina principal per a tots els centres de Catalunya, ja que els Instituts d'Educació Secundària, Centre d'Educació Infantil i Primària i Centre de Formació de persones Adultes l'utilitzen per a gestionar el seu centre. Dins d'aquest programa hi trobem les dades d'alumnes, les dades de professors, les dades del PAS (Personal d'administració i serveis), s'hi gestionen les faltes dels alumnes, les dades econòmiques per part de la direcció del centre, entre d'altres.

A nosaltres ens interessen les dades del personal que roman al centre durant el curs acadèmic. Per tant, les dades que necessitem són el DNI (actua com a identificador d'usuari) i nom complet (separant el nom, 1r cognom i 2n cognom) del personal que romandrà en el centre durant el curs acadèmic actual.

Per tal de realitzar aquesta importació de dades hem de disposar d'un compte d'usuari que tingui accés a aquestes dades. En el nostre cas, el centre ens facilitarà els fitxers amb les dades del personal. Aquestes dades estaran separades en 3 grups, professorat, personal del PAS (Personal Administració i Serveis) i alumnes. D'aquesta manera tindrem agrupats els 3 tipus de personal que conviuran al centre. És important separar aquests grups ja que cadascun d'ells tindrà uns determinats permisos o accessos restringits a determinats serveis del centre.

2. Inserció de dades a la Intra web i Moodle.

En l'apartat anterior hem obtingut les dades de tot el personal que romandrà en el centre. Ara ja podem utilitzar les dues plataformes web

que utilitza el centre per tal de començar el procés d'alta d'usuaris als serveis del centre.

L'aplicació web que ens serveix per a fer el primer pas és la Intraweb. "Aquesta Intraweb va néixer amb l'objectiu d'aprofitar les possibilitats i recursos que ofereixen les TIC per desenvolupar una eina que proporcionï mecanismes de comunicació en el centre, a la vegada que aportï solucions a problemes quotidians de la vida escolar.

El resultat ha estat una eina interactiva, participativa, accessible via Internet i fàcil de gestionar, on tots els col·lectius del centre poden trobar i aportar informació. Aquesta eina també ha de dotar el professorat de recursos per a l'ensenyament TIC, ajudant d'aquesta manera l'alumnat a assolir les competències bàsiques en aquest àmbit."

La Intraweb ja incorpora un mòdul d'importació i exportació d'usuaris que ens permet, a partir de fitxers .csv, realitzar l'alta dels usuaris al servei web i generar, de forma automàtica, els username (noms d'usuari) i password (contrasenya) dels usuaris del sistema. Per tant, a partir de la informació exportada del sistema SAGA, ja podem donar d'alta a tot el personal al servei web Intraweb. Caldrà validar-nos com administradors.

- Accés al mòdul d'administració d'usuaris

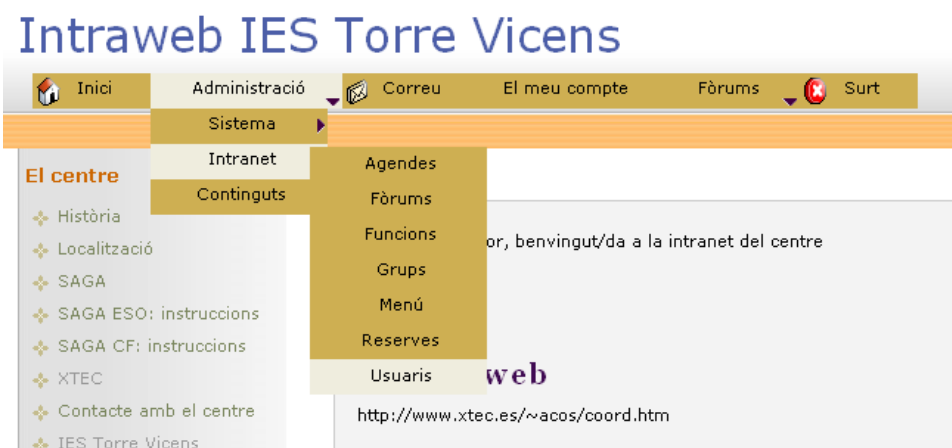


Figura 58: Accés al mòdul d'administració de la Intraweb.

- Pàgina principal del mòdul d'administració d'usuaris.



Figura 59: Pàgina de gestió d'usuaris de la Intraweb.

Nosaltres volem fer la importació del usuaris que hem extret de SAGA. Per a que això sigui possible, el fitxer de importació (en aquest cas un .csv) ha de contenir una sèrie de camps ja definits. Per conèixer aquests camps, primerament podem fer una exportació dels usuaris actuals (els que venen per defecte amb la instal·lació de la Intraweb. D'aquesta forma sabrem els camps dels que ha disposar el nostre fitxer de importació.

- Mostra d'un fitxer exportat amb els camps requerits.

#	id	Nom	cognom1	cognom2	nom_u	contrasenya	grup
1	12345678C	Aaaa	Cogaaa1	Coaaa2			4
2	98765432B	Bbbb	Cogbbb1	Cobbb2			3

Figura 60: Format de la taula d'usuaris de la Intraweb.

En aquesta taula, els usuaris es separen entre Administradors, Alumnes, Personal del PAS i Professors mitjançant el camp **grup**.

Grup	Usuaris	Descripció
2	Administradors	Administradors de la Intraweb. Accés total a

		tots els mòduls de la IntraWeb.
3	Professors	Professors del centre amb accés a altres recursos dins la IntraWeb.
4	Alumnes	Alumnes del centre
5	PAS	Personal d'Administració i Serveis.

Figura 61: Aclaració sobre els grups d'usuaris de la IntraWeb.

Com que des d'un principi el grup d'administradors ja està creat i ja hi tenim l'usuari administrador (admin), només ens farà falta importar els 3 grups d'usuaris que hem extret de SAGA. .

Si comparem la taula extreta de SAGA i la taula que conté els camps necessaris per a la exportació, veiem que els camps "nom_u" i "contrasenya" són buits. Aquests camps els generarà automàticament el gestor d'usuaris de la IntraWeb, per tant, no ens hem de preocupar del fet que hi hagi usuaris duplicats, ja que tot això ho controlarà el propi gestor. De totes maneres, haurem de retocar (com que és senzill ho farem de forma manual) el fitxer exportat de SAGA per tal de que compleixi els requisits per a la importació des de la IntraWeb. Haurem d'afegir de forma manual la capçalera de tres columnes més que correspondran als camps: nom_u, contrasenya i grup respectivament. Cal que els identificadors de les columnes (tuples) estiguin exactament escrites d'aquesta forma:

Format: (#, id, nom, cognom1, cognom2, nom_u, contrasenya, grup)

Els camps nom_u i contrasenya els generarà el gestor automàticament. El camp que si que haurem d'editar és el grup, ja que en aquest moment (amb el fitxer dades obert), ens és molt fàcil afegir el numero de grup al que fa referència al l'usuari. En tindrem prou en escriure el valor de grup i "arrastrar" el valor al llarg de la columna "grup".

Un cop fetes aquestes petites modificacions, ja estarem en disposició de realitzar la importació d'usuaris a la IntraWeb. Seguirem els passos que ens marca el gestor.

Per a començar a realitzar la importació dels usuaris, anem a l'opció: "Importació dades des d'un fitxer". Ens apareixerà la següent pantalla:

Intraweb IES Torre Vicens

Usuaris

[Afegeix un usuari/ària nou](#) [Mostra la llista d'usuaris/àries](#) [Importa dades des d'un fitxer](#) [Exporta a un fitxer CSV](#)

Importa dades des d'un fitxer
Primer pas: tria de l'arxiu XML o CSV

[Pel que fa a aquest mòdul](#)

Figura 62: Inici del procés d'importació.

Seleccionem l'opció “Examinar” i seleccionem els fitxers exportats anteriorment. Seleccionem l'opció “Ves al pas 2”. Si el fitxer és correcte ens apareixerà la següent pantalla:

Intraweb IES Torre Vicens

Usuaris

[Afegeix un usuari/ària nou](#) [Mostra la llista d'usuaris/àries](#) [Importa dades des d'un fitxer](#) [Exporta a un fitxer CSV](#)

Importa dades des d'un fitxer
Segon pas: comprovació que el fitxer XML o CSV triat és correcte
 Fitxer d'origen de les dades: pas1.csv

Camps trobats en el fitxer XML o CSV

#	Correcte
id	Correcte
nom	Correcte
cognom1	Correcte
cognom2	Correcte
nom_u	Correcte
contrasenya	Correcte
grup	Correcte

S'han trobat 14 registre/s

S'han recuperat les dades satisfactòriament. Podeu continuar amb el tercer pas.

Figura 63: Primer pas d'importació realitzat correctament.

Seleccionem l'opció “Ves al pas 3”. Apareixerà la següent pantalla. En ella haurem de gestionar els usuaris nous que hem importat. Seleccionarem l'opció “Gestiona els usuaris/àries que són a la taula d'importació i no a la de la Intranet”. Vegeu següent figura:

Intraweb IES Torre Vicens

[Inici](#) [Administració](#) [Correu](#) [El meu compte](#) [Fòrums](#) [Surt](#)

Usuaris

[Afegeix un usuari/ària nou](#)

[Mostra la llista d'usuaris/àries](#)

[Importa dades des d'un fitxer](#)

[Exporta a un fitxer CSV](#)

Importa dades des d'un fitxer

Tercer pas: sincronització de les taules

Tria l'acció que vols dur a terme:

[Gestiona els usuaris/àries que són a les dues taules, però que tenen diferències en les dades](#)

0 registre/s

[Cancel·la els canvis](#)

[No facis cap acció](#)

[Gestiona els usuaris/àries que són a la taula d'importació i no a la de la intranet](#)

14 registre/s

[Cancel·la els canvis](#)

[No facis cap acció](#)

[Gestiona els usuaris/àries que són a la taula de la intranet i no a la d'importació](#)

10 registre/s

[Cancel·la els canvis](#)

[No facis cap acció](#)

[Gestiona els usuaris/àries que són a la taula d'importació i no a la de la intranet](#)

[Repasa i executa les ordres donades](#)

0 registre/s

En el fitxer d'importació d'usuaris/àries teniu 14 registre/s per gestionar

A la taula d'usuaris/àries de la intranet teniu 10 registre/s per gestionar

Web creada amb [PostNuke](#) - Adreça del centre - codi postal i població - [Contacteu amb el centre](#)

Figura 64: Gestió dels usuaris importats.

En la següent figura es mostra la pantalla on ja s'han generat els noms d'usuari i contrasenyes del personal. Si tot és correcte, en el següent pas només haurem de repassar i executar les ordres i aquests usuaris ja formaran part de la Intraweb. Seleccionarem l'opció "Continua".

Importa dades des d'un fitxer**Tercer pas: sincronització de les taules**

Gestiona els usuaris/àries que són a la taula d'importació i no a la de la intranet

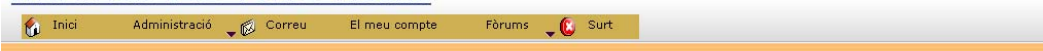
Els usuaris/àries següents només són a la taula d'importació d'usuaris/àries. En cada cas, trieu l'opció més oportuna

Nom	1r cognom	2n cognom	Opció	Per a l'opció "crea l'usuari/ària" trieu un nom d'usuari, un grup i una contrasenya		Per a l'opció "Associa a l'usuari/ària" trieu a quin usuari/ària el voleu associar
Monica	Coscolluela	Campo	Crea l'usuari/ària	mcoscoll mc2360	Alumnat	Administrador
Raya	Eltayeb	Almacellas	Crea l'usuari/ària	reltayeb re5116	Alumnat	Administrador
Sheila	Lopez	Gallardo	Crea l'usuari/ària	slopez sl4278	Alumnat	Administrador
Veronica	Rius	Rodriguez	Crea l'usuari/ària	vrrius vr1271	Alumnat	Administrador
Laura	Olivella	Sanz	Crea l'usuari/ària	lolivell lo3328	Alumnat	Administrador
Miriam	Garsaball	Royo	Crea l'usuari/ària	mrgarsaba mg4844	Alumnat	Administrador
Ingrid	Burgos	Gomez	Crea l'usuari/ària	iburgos ib2895	Alumnat	Administrador
Gemma	Duart	Bosch	Crea l'usuari/ària	gduart gd9113	Alumnat	Administrador
Angel	Camacho	Puerto	Crea l'usuari/ària	acamacho ac8937	Alumnat	Administrador
Maria	Solà	Cortada	Crea l'usuari/ària	msola ms1638	Alumnat	Administrador
Florencia del Pilar	Retamoso	Viera	Crea l'usuari/ària	frretamos fr1419	Alumnat	Administrador
Mónica	Roe	Canillo	Crea l'usuari/ària	mroge	Alumnat	Administrador

Figura 65: Confirmació de les dades de connexió dels usuaris.

En la següent pantalla seleccionem “repassa i executa les ordres donades”.

Intraweb IES Torre Vicens



Usuaris

[Afegeix un usuari/ària nou](#)

[Mostra la llista d'usuaris/àries](#)

[Importa dades des d'un fitxer](#)

[Exporta a un fitxer CSV](#)

Importa dades des d'un fitxer

Tercer pas: sincronització de les taules

Tria l'acció que vols dur a terme:

[Gestiona els usuaris/àries que són a les dues taules, però que tenen diferències en les dades](#)

[Gestiona els usuaris/àries que són a la taula d'importació i no a la de la intranet](#)

[Gestiona els usuaris/àries que són a la taula de la intranet i no a la d'importació](#)

0 registre/s

[Cancel·la els canvis](#)

[No facis cap acció](#)

0 registre/s

[Cancel·la els canvis](#)

[No facis cap acció](#)

10 registre/s

[Cancel·la els canvis](#)

[No facis cap acció](#)

...

14 registre/s

[Repassa i executa les ordres donades](#)

En el fitxer d'importació d'usuaris/àries [Repassa i executa les ordres donades](#) pr
A la taula d'usuaris/àries de la intranet teniu 10 registre/s per gestionar

Figura 66: Repàs de les ordres donades.

Ens apareixerà la següent pantalla. Aquest apartat mostra un resum de les tasques que es duran a terme en el següent pas. En cas de que hi haguessin usuaris repetits, durant aquest procés ja els hauríem detectat i ja hauríem pogut modificar les dades connexió. Si tot està correcte seleccionem "Continua".

Importa dades des d'un fitxer
Tercer pas: sincronització de les taules
 Repassa i executa les ordres donades

Acció que es durà a terme	Opció
Alta a la intranet L'usuari/ària Monica Cosculluela Campo serà donat d'alta a la intranet amb el nom d'usuari mcoscull dins del grup Alumnat	Descarta
Alta a la intranet L'usuari/ària Raya Eltayeb Almacellas serà donat d'alta a la intranet amb el nom d'usuari reltayeb dins del grup Alumnat	Descarta
Alta a la intranet L'usuari/ària Sheila Lopez Gallardo serà donat d'alta a la intranet amb el nom d'usuari slopez dins del grup Alumnat	Descarta
Alta a la intranet L'usuari/ària Veronica Rius Rodriguez serà donat d'alta a la intranet amb el nom d'usuari vrius dins del grup Alumnat	Descarta
Alta a la intranet L'usuari/ària Laura Olivella Sanz serà donat d'alta a la intranet amb el nom d'usuari lolivell dins del grup Alumnat	Descarta
Alta a la intranet L'usuari/ària Míriam Garsaball Royo serà donat d'alta a la intranet amb el nom d'usuari mgarsaba dins del grup Alumnat	Descarta
Alta a la intranet L'usuari/ària Ingrid Burgos Gomez serà donat d'alta a la intranet amb el nom d'usuari iburgos dins del grup Alumnat	Descarta
Alta a la intranet L'usuari/ària Gemma Duart Bosch serà donat d'alta a la intranet amb el nom d'usuari gduart dins del grup Alumnat	Descarta
Alta a la intranet L'usuari/ària Angel Camacho Puerto serà donat d'alta a la intranet amb el nom d'usuari acamacho dins del grup Alumnat	Descarta
Alta a la intranet L'usuari/ària Maria Solà Cortada serà donat d'alta a la intranet amb el nom d'usuari msola dins del grup Alumnat	Descarta
Alta a la intranet L'usuari/ària Florencia del Pilar Retamoso Viera serà donat d'alta a la intranet amb el nom d'usuari fretamos dins del grup Alumnat	Descarta
Alta a la intranet L'usuari/ària Mónica Roge Canillo serà donat d'alta a la intranet amb el nom d'usuari mroge dins del grup Alumnat	Descarta
Alta a la intranet L'usuari/ària Tamara Trujillano Heredia serà donat d'alta a la intranet amb el nom d'usuari ttrujill dins del grup Alumnat	Descarta
Alta a la intranet L'usuari/ària Raquel Celma Bellera serà donat d'alta a la intranet amb el nom d'usuari rcelma dins del grup Alumnat	Descarta

Queden 14 registres per gestionar en aquest apartat

[Continua >>](#)

Figura 67: Confirmació de la inserció dels usuaris a la IntraWeb.

Un cop importats aquest usuaris centrarem l'atenció en dues taules de la base de dades de la IntraWeb. Accedirem a aquestes taules a través del gestor de bases de dades PhpMyAdmin [25]. La taules són:

- iw_nuke_detic_usuaris_saga
- iw_nuke_users

La primera conté les dades dels alumnes que hem importat incloses les dades de connexió (nom d'usuari i contrasenya (en clar)). Per tant d'aquesta taula extraurem les dades de connexió que haurem de facilitar als usuaris.

Per altra banda, la taula iw_nuke_users contindrà més camps que l'anterior però d'aquesta taula no podem extreure les dades de connexió

dels usuaris ja que el camp "pn_pass" corresponent a la contrasenya de l'usuari ja ha estat xifrat amb MD5 [26] (format hexadecimal).

Ara necessitem adaptar les dades extretes de la base de dades al format de dades necessari per a realitzar la importació de dades al servei LDAP.

El Servei LDAP disposa de camps que encara no podem omplir perquè no disposem de les dades necessàries. Aquests camps són els password xifrats amb MD5 i els de passwords de SAMBA (SambaLTPassword i SambaMTPassword), i també els identificadors del domini, entre d'altres. Per tant, cal crear una petita aplicació que reestructuri les dades que si que tenim per a poder-les tractar després. Amb la taula extreta de la base de dades tenim el password en clar dels usuaris, per tant, a partir d'aquesta dada podem crear les dades que ens falta.

Per adaptar el fitxer de dades a les nostres necessitats utilitzarem la comanda "cut", que ens agafarà només les dades necessàries i ens les guardarà en un fitxer anomenat users.csv.

Comanda amb cut:

```
#cut -d " , " -f4, 5, 9, 10 iw_nuke_deti c_usuari s_saga.csv  
> users.csv
```

Ens crearà el fitxer: users.csv (que contindrà totes les dades necessàries i ordenades per a poder-les tractar i generar posteriorment el fitxer d'importació final.)

En aquest moment només ens falta canviar de format de fitxer, és a dir, hem de canviar el format .csv al format .ldif per a poder realitzar la importació dels usuaris des del servei LDAP mitjançant el PhpLDAPAdmin. A més també hem d'afegir els camps que fan referència al nom de domini, identificadors de domini, etc, ... Aquest camps els escriurem directament en el programa de canvi de format. Ho fem així perquè un cop configurat el nom domini i creat el identificador, aquests no canviaran fins que no reinstal·lem el servidor o afegim més controladors de domini.

El següent script ens realitzarà aquest canvi de format i estructura de fitxer:

Codi del script:

```
#!/usr/bin/perl

use Digest::MD5;
use MIME::Base64;

open (LDIF, "+>. /users.ldif");
$csv = @ARGV[0];
open (CSV, "$csv");

$uidNumber=10010;

while ($line = <CSV>)
{
    chomp $line;

    ($givenName, $sn, $userPassword, $uid) = split ("", $line);

    $ctx = Digest::MD5->new;
    $ctx->add($userPassword);
    $hashedPasswd = '{MD5}' . encode_base64($ctx->digest,);

    my $sambaLM = (`mkntpwd -L $userPassword`);
    my $sambaNT = (`mkntpwd -N $userPassword`);

    printf LDIF ("%s", "dn: cn=$givenName $sn,ou=users,dc=intracentre\n");
    printf LDIF ("%s", "givenName: $givenName\n");
    printf LDIF ("%s", "sn: $sn\n");
    printf LDIF ("%s", "cn: $givenName $sn\n");
    printf LDIF ("%s", "uid: $uid\n");
    printf LDIF ("%s", "userPassword: $hashedPasswd");
    printf LDIF ("%s", "SambaLMPassword: $sambaLM");
    printf LDIF ("%s", "SambaNTPassword: $sambaNT");
    printf LDIF ("%s", "gidNumber: 20001\n");
    printf LDIF ("%s", "SambaPrimaryGroupSID: I denti fi cadorsamba-513-\n");
    printf LDIF ("%s", "homeDirectory: /home/$uid\n");
    printf LDIF ("%s", "sambaAcctFlags: [U]\n");
    printf LDIF ("%s", "objectClass: inetOrgPerson\n");
    printf LDIF ("%s", "objectClass: SambaSamAccount\n");
    printf LDIF ("%s", "objectClass: posixAccount\n");
    printf LDIF ("%s", "objectClass: top\n");
    printf LDIF ("%s", "SambaSID: I denti fi cadorsamba-513\n");
    printf LDIF ("%s", "uidNumber: $uidNumber\n\n");

    $uidNumber++;
}
close CSV;
exit (0);
```

Comanda per l'execució de l'script:

```
#perl csvalldif.pl users.csv
```

Ens crearà el fitxer: users.ldif

Aquest últim fitxer és el que importarem des del phpLDAPAdmin.

Per poder realitzar una correcta conversió del fitxer users.csv, abans cal fer una modificació en aquest fitxer, ja que si executem el script de conversió de format amb el fitxer creat al primer pas (adaptació de dades per a la importació), es crearà un fitxer de dades erroni (users.ldif). Aquest fitxer serà erroni perquè els paràmetres referents al usuari estaran remarcats entre "" (cometes dobles) i això donarà problemes a l'hora d'importar el fitxer des de PhpLDAPAdmin.

Per solucionar aquest petit entrebanc utilitzarem la comanda "sed" amb els paràmetres corresponents per tal d'eliminar les "" (cometes dobles) del fitxer creat amb la comanda "cut".

Comanda amb "sed":

```
#sed 's/"//g' temp.csv > users.csv;
```

Aquesta comanda agafarà el fitxer creat en el primer pas (temp.csv) i eliminarà les "" (cometes dobles) que conté. Finalment guardarà el fitxer com "users.csv". Aquest fitxer ja estarà preparat per tornar a ser tractat amb el script: "csvaldif.pl".

Pel que fa al servei web Moodle, només ens caldrà instal·lar l'entorn al servidor web del que disposem i aprofitar la mateixa taula d'usuaris de la Intraweb, ja que tots dos serveis comparteixen, a part de mòduls que faciliten la integració de les dues plataformes, els noms d'usuari i les contrasenyes.

Moodle es defineix com un entorn web d'aprenentatge on professors i alumnes interactuen amb la realització de diferents tipus de tasques i activitats, amb una sèrie de grans avantatges i facilitats.

Segons la wikipedia:

"Moodle" és un programari de codi lliure que crea entorns virtuals d'ensenyament i aprenentatge.

El projecte fou iniciat, i és mantingut, per l'australià Martin Dougiamas. Però ha aconseguit reunir una gran comunitat internacional d'usuaris, programadors, desenvolupadors i traductors de tal forma que actualment té 75.000 usuaris registrats i està traduït a 75 llengües, inclòs el català.

La clau del seu èxit rau en la facilitat d'instal·lació (només necessita un servidor php i una base de dades com MySQL), de configuració, creació

de cursos i manteniment del lloc. Està construït sota una òptica de construcció del coneixement basat en el diàleg entre els participants, el constructivisme social. Per això és tan fàcil crear-hi fòrums. Tot i això accepta molts altres tipus d'activitats didàctiques: qüestionaris, lliçons, tasques, wikis, xats, etc.

Filosofia

El disseny i desenvolupament de Moodle es basen en la idea de la *pedagogia construccionista social*. Aquesta filosofia radica en la cooperació en grup i en la idea de que el coneixement es pot crear o construir.

Com a curiositat, cal fer menció que Moodle és la primera comunitat Open Source no formada íntegrament per informàtics, sinó que també participen pedagogs i altra gent relacionada amb l'ensenyament.

Característiques

- Promou la pedagogia constructivista social.
- Es poden fer les classes 100% en línia.
- Té una interfície senzilla, lleugera i molt intuïtiva.
- Instal·lable en qualsevol plataforma que suporti PHP (només requereix l'existència d'una base de dades).
- Ofereix un llistat dels cursos amb descripcions i la possibilitat d'entrar-hi com a usuari convidat.
- Seguretat ben sòlida, els formularis es revisen, les cookies s'encripten.
- El tema de la interfície és altament personalitzable.
- Els paquets d'idioma permeten localitzar a qualsevol idioma per complet (75 idiomes).
- Inclou diversos mòduls per a tallers, fòrums, consultes, xats, etc.
- Alta Disponibilitat.
- Escalabilitat.
- Fàcil ús.
- Interoperable.
- Estable.
- Segur.”

3. Importació de dades al Servidor PDC.

Per fer-ho accedim al PhpLdapAdmin:

<https://pdc/phpldapadmin/>

Ens validem com administradors i accedim a l'opció: import.

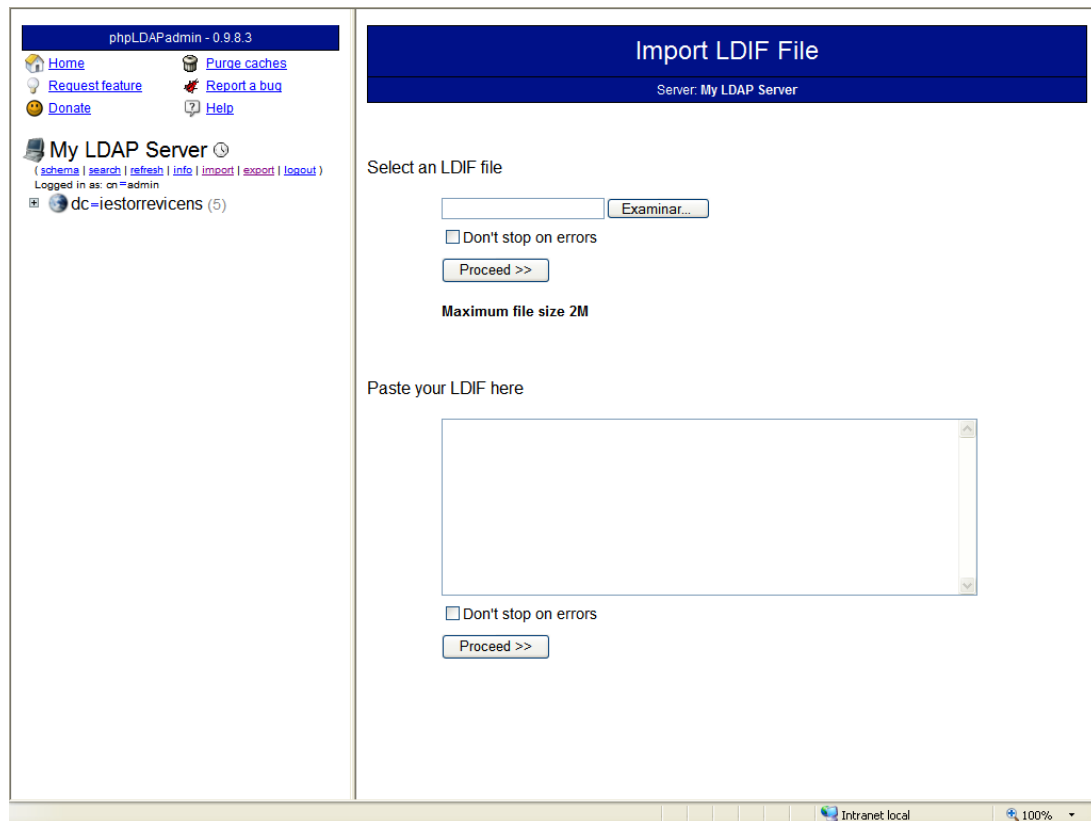


Figura 68: Pàgina d'importació de dades al Servei LDAP.

Seleccionarem l'opció "Examinar" i busquem el nostre fitxer: users.ldif.

Un cop trobat seleccionem l'opció "Proceed". Si tot ha anat be ja tindrem donats d'alta a tots els usuaris dins del contenidor users del directori LDAP.

4. Automatització de creació del directoris d'usuaris.

En aquest apartat farem ús d'un script que ens permetrà consultar la base de dades LDAP i crear i/o esborrar els directoris d'usuaris existents i/o inexistents. Per crear els directoris dels usuaris caldrà saber quins usuaris estan donats d'alta al sistema, a quin grup pertanyen aquest usuaris i si ja tenen o no un directori propi on emmagatzemar les seves dades.

L'script reb el nom de makedelhomes.sh i conté el següent codi font:

```

#!/bin/sh
#Contrasenya de connexio al servidor ldap
systempass="password"
# Bind dn
bi nddn="cn=admin,dc=intracentre"
# Account leave
accountleave="ou=users,dc=intracentre"
# nom del ordinador on esta instal·lat el servei ldap
ldaphost="localhost"
# skel directory
skel="/etc/skel/"
# Directori arrel dels usuaris
homeleave="/home"

usernames=`ldapsearch -h $ldaphost -x -w $systempass -D "$bi nddn" \
-b "$accountleave" uid | grep "^[^#]" | grep "^[^dn]" \
| grep uid | awk '{ print $2 }'`

# creacio dels directoris personals

for username in $usernames
do
    homedirectory=`ldapsearch -h $ldaphost -x -w $systempass -D "$bi nddn" \
-b "$accountleave" "(uid=$username)" homeDirectory \
| grep "^[^#]" | grep homeDirectory \
| awk '{ print $2 }'`

    group=`ldapsearch -h $ldaphost -x -w $systempass -D "$bi nddn" \
-b "$accountleave" "(uid=$username)" gidNumber \
| grep "^[^#]" | grep gidNumber \
| awk '{ print $2 }'`

    if [ ! -d $homedirectory ] && [ ! -z $homedirectory ]
    then

        cp -a $skel $homedirectory
        chown -R $username.$group $homedirectory
    fi

done

# eliminacio dels directoris personals

for username in `ls $homeleave`
do
    name=`ldapsearch -h $ldaphost -x -w $systempass -D "$bi nddn" \
-b "$accountleave" "(homeDirectory=$homeleave/$username)" uid \
| grep "^[^#]" | grep "uid:" | awk '{ print $2 }'`

    if [ -z $name ]
    then
        rm -rf $homeleave/$username
    fi
done

```

5. Menú d'administració del sistema.

En aquest apartat crearem un menú amb shell script que ens permetrà realitzar les tasques d'administració abans esmentades d'una forma més fàcil i automatitzada.

Aquest executarà els scripts creats fins al moment, d'aquesta forma farem més usable la implantació del sistema.

El menú disposarà de les següents opcions:

1. Adapatacio dels usuaris de la Inraweb al format LDAP.
2. Creacio del fitxer d'importacio a LDAP (users.ldif).
3. Creacio dels Home d'usuari.
4. Eliminacio dels directoris d'usuaris no registrats.
5. Sortir. Sortir del menú d'administració.

L'Script de l'apartat 4 d'aquest capítol s'ha separat en dos opcions en el Menú d'administració per tal de no esborrar, al menys, en aquell mateix moment, el directori de l'usuari que s'ha donat de baixa de la base de dades LDAP.

Codi font del Menú d'administració:

```
#!/bin/bash
# Per fer us correctament d'aquest script cal tenir instal·lat el
# següent programari:
# mkntpwd (http://www.silcom.com.pe/soft/mkntpwd.tar.gz),
# make, gcc, gcc++, gengetopt, libpopt-dev, python-crypto.

while :
do
clear
echo "  MENU D'ADMINISTRACIO  "
echo "1. Adapatacio dels usuaris de la Intraweb al format LDAP"
echo "2. Creacio del fitxer d'importacio a LDAP (users.ldif)"
echo "3. Creacio dels Home d'usuari"
echo "4. Eliminacio dels directoris d'usuaris no registrats"
echo "5. Sortir"
echo -n "Si us plau, escull una de les opcions anteriors [1 - 5]: "
read opt
case $opt in
1) echo "1. Adapatacio dels usuaris de la Intraweb al format LDAP"
cut -d "," -f4,5,9,10 iw_nuke_detic_usuaris_saga.csv > temp.csv;
sed 's/"//g' temp.csv > users.csv;
rm temp.csv;
echo "Prem la tecla [enter] per continuar. . .";
read enterKey;;
2) echo "2. Creacio del fitxer d'importacio a LDAP (users.ldif)";
perl csvldif.pl users.csv;
echo "Prem la tecla [enter] per continuar. . .";
read enterKey;;
3) echo "3. Creacio dels Home d'usuari";
sh crearhome.sh;
echo "Prem la tecla [enter] per continuar. . .";
read enterKey;;
4) echo "4. Eliminacio dels directoris d'usuaris no registrats";
sh borrarhome.sh;
echo "Prem la tecla [enter] per continuar. . .";
read enterKey;;
5) echo "5. Sortir.";
exit 1;;
*) echo "$opt Opcio invalida. Si us plau, selecciona una opcio entre
1-5";
echo "Prem la tecla [enter] per continuar. . .";
read enterKey;;
esac
done
```


Capítol 8: Conclusions.

Una cop hem arribat al final de la realització del projecte creiem que s'han complert la majoria dels objectius de forma satisfactòria, ja que després de tot aquest temps de treball i estudi s'ha arribat a crear una eina que compleix els requisits marcats inicialment.

Aquest treball s'ha convertit per una banda en una eina de consulta per part del centre educatiu, ja que en ella hi trobaran totes les respostes de configuració i funcionament dels serveis que s'ha ficat en funcionament, i per altra banda, en una síntesi de tot el que he après i aplicat durant l'elaboració d'aquest projecte.

He de recalcar que ha estat una feina dura i constant, ja que a part d'haver d'adquirir nous coneixements per la implantació dels serveis, també havia de pensar com fer-ho de la forma més senzilla possible, donat que els usuaris finals d'aquest sistema són gent amb coneixements informàtics no avançats, i que per tant, la senzillesa havia de ser la premissa bàsica de l'elaboració d'aquest projecte.

El fet d'estar amb contacte amb el personal del centre ha propiciat un feedback molt positiu entre el personal del centre en qüestió i jo mateix. Aquesta retroalimentació i bona sintonia entre els membres de la coordinació informàtica i equip directiu del centre ha propiciat adaptar de la millor manera possible el projecte que s'estava fent a les necessitats reals del centre, cuidant cada detall, buscant-ne els pros i els contres i sempre buscant la solució més adequada basant-nos amb els principis establerts (veieu pàgina 18).

Pel que fa als objectius assolits podem dir que:

- S'ha creat una guia d'instal·lació i configuració clara i molt pautada que permetrà als responsables del centre en qüestió a entendre el funcionament dels serveis instal·lats, mantenir-los i/o ampliar-los en un futur.
- S'ha ficat en funcionament un sistema que es capaç de respondre a les necessitats del centre, i a més donant la possibilitat d'ampliar aquests serveis. Per tot això s'ha utilitzat un programari

molt estable que garantirà el correcte funcionament del sistema i dotarà al centre de la tranquil·litat necessària per a que només s'hagi de preocupar de gaudir d'aquest serveis i de respondre a les noves necessitats que aniran arribant.

- A més de donar solució a les problemàtiques inicials i a l'establiment dels nous serveis, s'ha creat i s'han donat les premisses bàsiques de "com" crear un Live CD que ens faciliti les tasques d'instal·lació, manteniment i restauració del sistema. El resultat de la creació d'aquest Live CD no ha estat el desitjat ja que han quedat en l'aire alguns problemes dels quals encara no s'hi ha trobat la solució i que per tant, queden com a projectes futurs o millores que caldrà realitzar en un futur.
- Per últim s'ha creat una aplicació capaç de gestionar les dades dels usuaris d'una forma molt simple i simplificada que permetrà als administradors del sistema donar d'alta al personal del centre d'una forma ràpida i amb les màximes facilitats possibles.

Aquest treball de fi de carrera m'ha servit per introduir-me molt més en el món del programari lliure, i especialment, a la implantació de serveis relacionats amb xarxes de comunicació. El fet d'haver assolit tots aquest conceptes relacionats amb les xarxes crec que m'obre un món molt extens, amb infinitat de conceptes per aprendre i millorar, i el que és també important, m'ha ajudat a estar preparat de cara a la inserció laboral, ja que tots aquest serveis implantats són la base que sustenta moltes empreses, no només les de caire informàtic i tecnològic, sinó qualsevol empresa que necessita d'aquests serveis per a crear una estructura de treball que els permeti assolir els seus objectius.

Tots aquests conceptes relacionats amb les xarxes de comunicació parteixen de la base assolida durant els estudis de l'enginyeria, tant de l'assignatura de xarxes com del bloc optatiu d'Internet, sense menys prear, es clar, la resta d'assignatures impartides, que en major o menor mesura també m'han servit com a base per a assolir nous conceptes o per aplicar-ne els ja adquirits durant els estudis.

Val a dir també que de cadascun dels serveis que s'ha posat en funcionament gairebé en sortiria un altre treball de fi de carrera, ja que són serveis amb infinitat de variables i possibles configuracions. En el nostre cas però, hem utilitzat la base de tots aquests serveis per a implantar un sistema que ens ajudi a complir els objectius marcats des d'un principi.

M'agradaria fer esment de que aquest projecte es va iniciar amb una idea una mica diferent de la que finalment s'ha dut a terme. El fet de saber ben bé el que necessitava el centre i com portar-ho a terme de la forma més fàcil possible han estat els principals “cavalls de batalla” del projecte. Estava clar des d'un principi que calia elaborar un projecte molt pautat i amb les màximes facilitats de posada en funcionament. Finalment, la idea inicial s'ha anat polint per arribar al treball que tenim a les mans.

Capítol 9: Treballs futurs.

En aquest apartat sobre treballs futurs donaré a conèixer les possibilitats d'expansió i/o millora del treball actual, ja que sóc conscient de que aquest treball de fi de carrera no acaba aquí, sinó que com la majoria de treballs o projectes, poden ampliar-se i millorar-se en major o menor mesura.

- Accés a l'espai de treball dels usuaris de forma remota. És a dir, que els usuaris puguin accedir a les seves dades des d'un punt de connexió extern al centre. Caldria establir una configuració dels equips tallafocs i del servidor per tal de que els usuaris del centre es poguessin connectar des de qualsevol lloc extern al centre educatiu.
- Resolució dels problemes que s'ha tingut durant la creació del Live CD i creació definitiva d'un "cd viu" que ens faciliti al màxim el procés d'implantació d'un Servidor PDC.
- Crear un menú d'administració del sistema més atractiu i que ens faciliti l'ús des d'altres plataformes com per exemple una pàgina web.
- Implantar les eines de monitorització necessàries per a tenir un control exhaustiu del Servidor en tot moment.
- Fer possible la implantació dels serveis en un entorn que ja està en producció, és a dir, sense conèixer les contrasenyes dels usuaris, poder generar les dades de connexió necessàries per a donar als usuaris existents l'alta als nous serveis implantats.
- Personalització de scripts d'inici per a cada usuari de la xarxa en funció del grup al qual pertanyen.
- Adaptació del sistema a la implantació del Projecte HEURA d'ensenyament, adaptant les configuracions del sistema per a donar suport a la nova estructura de xarxa a la que es sotmetrà el centre. Per més informació sobre el projecte heura:

http://www.xtec.cat/at_usuari/guies/heura/configuracio_centres/

Annex.

Llicència GPL

En aquest annex podeu trobar la llicència GPL. Aquesta llicència és la que he utilitzat per aquest treball. La llicència està en anglès, la seva versió oficial, ja que no es reconeixen com a oficials les traduccions a altres llengües. El motiu d'això es que examinar tots els textos traduïts seria massa costós i difícil.

GNU GENERAL PUBLIC LICENSE

Version 3, 29 June 2007

Copyright © 2007 Free Software Foundation, Inc. <<http://fsf.org/>>

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The GNU General Public License is a free, copyleft license for software and other kinds of works.

The licenses for most software and other practical works are designed to take away your freedom to share and change the works. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change all versions of a program--to make sure it remains free software for all its users. We, the Free Software Foundation, use the GNU General Public License for most of our software; it applies also to any other work released this way by its authors. You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for them if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs, and that you know you can do these things.

To protect your rights, we need to prevent others from denying you these rights or asking you to surrender the rights. Therefore, you have certain responsibilities if you distribute copies of the software, or if you modify it: responsibilities to respect the freedom of others.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must pass on to the recipients the same freedoms that you received. You must make

sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

Developers that use the GNU GPL protect your rights with two steps: (1) assert copyright on the software, and (2) offer you this License giving you legal permission to copy, distribute and/or modify it.

For the developers' and authors' protection, the GPL clearly explains that there is no warranty for this free software. For both users' and authors' sake, the GPL requires that modified versions be marked as changed, so that their problems will not be attributed erroneously to authors of previous versions.

Some devices are designed to deny users access to install or run modified versions of the software inside them, although the manufacturer can do so. This is fundamentally incompatible with the aim of protecting users' freedom to change the software. The systematic pattern of such abuse occurs in the area of products for individuals to use, which is precisely where it is most unacceptable. Therefore, we have designed this version of the GPL to prohibit the practice for those products. If such problems arise substantially in other domains, we stand ready to extend this provision to those domains in future versions of the GPL, as needed to protect the freedom of users.

Finally, every program is threatened constantly by software patents. States should not allow patents to restrict development and use of software on general-purpose computers, but in those that do, we wish to avoid the special danger that patents applied to a free program could make it effectively proprietary. To prevent this, the GPL assures that patents cannot be used to render the program non-free.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS

0. Definitions.

“This License” refers to version 3 of the GNU General Public License.

“Copyright” also means copyright-like laws that apply to other kinds of works, such as semiconductor masks.

“The Program” refers to any copyrightable work licensed under this License. Each licensee is addressed as “you”. “Licensees” and “recipients” may be individuals or organizations.

To “modify” a work means to copy from or adapt all or part of the work in a fashion requiring copyright permission, other than the making of an exact copy. The resulting work is called a “modified version” of the earlier work or a work “based on” the earlier work.

A “covered work” means either the unmodified Program or a work based on the Program.

To “propagate” a work means to do anything with it that, without permission, would make you directly or secondarily liable for infringement under applicable copyright law, except executing it on a computer or modifying a private copy. Propagation includes copying, distribution (with or without modification), making available to the public, and in some countries other activities as well.

To “convey” a work means any kind of propagation that enables other parties to make or receive copies. Mere interaction with a user through a computer network, with no transfer of a copy, is not conveying.

An interactive user interface displays “Appropriate Legal Notices” to the extent that it includes a convenient and prominently visible feature that (1) displays an appropriate copyright notice, and (2) tells the user that there is no warranty for the work (except to the extent that warranties are provided), that licensees may convey the work under this License, and how to view a copy of this License. If the interface presents a list of user commands or options, such as a menu, a prominent item in the list meets this criterion.

1. Source Code.

The “source code” for a work means the preferred form of the work for making modifications to it. “Object code” means any non-source form of a work.

A “Standard Interface” means an interface that either is an official standard defined by a recognized standards body, or, in the case of interfaces specified for a particular programming language, one that is widely used among developers working in that language.

The “System Libraries” of an executable work include anything, other than the work as a whole, that (a) is included in the normal form of packaging a Major Component, but which is not part of that Major Component, and (b) serves only to enable use of the work with that Major Component, or to implement a Standard Interface for which an implementation is available to the public in source code form. A “Major Component”, in this context, means a major essential component (kernel, window system, and so on) of the specific operating system (if any) on which the executable work runs, or a compiler used to produce the work, or an object code interpreter used to run it.

The “Corresponding Source” for a work in object code form means all the source code needed to generate, install, and (for an executable work) run the object code and to modify the work, including scripts to control those activities. However, it does not include the work's System Libraries, or general-purpose tools or generally available free programs which are used unmodified in performing those activities but which are not part of the work. For example, Corresponding Source includes interface definition files associated with source files for the work, and the source code for shared libraries and dynamically linked subprograms that the work is specifically designed to require, such as by intimate data communication or control flow between those subprograms and other parts of the work.

The Corresponding Source need not include anything that users can regenerate automatically from other parts of the Corresponding Source.

The Corresponding Source for a work in source code form is that same work.

2. Basic Permissions.

All rights granted under this License are granted for the term of copyright on the Program, and are irrevocable provided the stated conditions are met. This License explicitly affirms your unlimited permission to run the unmodified Program. The output from running a covered work is covered by this License only if the output, given its content, constitutes a covered work. This License acknowledges your rights of fair use or other equivalent, as provided by copyright law.

You may make, run and propagate covered works that you do not convey, without conditions so long as your license otherwise remains in force. You may convey covered works to others for the sole purpose of having them make modifications exclusively for you, or provide you with facilities for running those works, provided that you comply with the terms of this License in conveying all material for which you do not control copyright. Those thus making or running the covered works for you must do so exclusively on your behalf, under your direction and control, on terms that prohibit them from making any copies of your copyrighted material outside their relationship with you.

Conveying under any other circumstances is permitted solely under the conditions stated below. Sublicensing is not allowed; section 10 makes it unnecessary.

3. Protecting Users' Legal Rights From Anti-Circumvention Law.

No covered work shall be deemed part of an effective technological measure under any applicable law fulfilling obligations under article 11 of the WIPO copyright treaty adopted on 20 December 1996, or similar laws prohibiting or restricting circumvention of such measures.

When you convey a covered work, you waive any legal power to forbid circumvention of technological measures to the extent such circumvention is effected by exercising rights under this License with respect to the covered work, and you disclaim any intention to limit operation or modification of the work as a means of enforcing, against the work's users, your or third parties' legal rights to forbid circumvention of technological measures.

4. Conveying Verbatim Copies.

You may convey verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice; keep intact all notices stating that this License and any non-permissive terms added in accord with section 7 apply to the code; keep intact all notices of the absence of any warranty; and give all recipients a copy of this License along with the Program.

You may charge any price or no price for each copy that you convey, and you may offer support or warranty protection for a fee.

5. Conveying Modified Source Versions.

You may convey a work based on the Program, or the modifications to produce it from the Program, in the form of source code under the terms of section 4, provided that you also meet all of these conditions:

- a) The work must carry prominent notices stating that you modified it, and giving a relevant date.
- b) The work must carry prominent notices stating that it is released under this License and any conditions added under section 7. This requirement modifies the requirement in section 4 to “keep intact all notices”.
- c) You must license the entire work, as a whole, under this License to anyone who comes into possession of a copy. This License will therefore apply, along with any applicable section 7 additional terms, to the whole of the work, and all its parts, regardless of how they are packaged. This License gives no permission to license the work in any other way, but it does not invalidate such permission if you have separately received it.
- d) If the work has interactive user interfaces, each must display Appropriate Legal Notices; however, if the Program has interactive interfaces that do not display Appropriate Legal Notices, your work need not make them do so.

A compilation of a covered work with other separate and independent works, which are not by their nature extensions of the covered work, and which are not combined with it such as to form a larger program, in or on a volume of a storage or distribution medium, is called an “aggregate” if the compilation and its resulting copyright are not used to limit the access or legal rights of the compilation's users beyond what the individual works permit. Inclusion of a covered work in an aggregate does not cause this License to apply to the other parts of the aggregate.

6. Conveying Non-Source Forms.

You may convey a covered work in object code form under the terms of sections 4 and 5, provided that you also convey the machine-readable Corresponding Source under the terms of this License, in one of these ways:

- a) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by the Corresponding Source fixed on a durable physical medium customarily used for software interchange.
- b) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by a written offer, valid for at least three years and valid for as long as you offer spare parts or customer support for that product model, to give anyone who possesses the object code either (1) a copy of the Corresponding Source for all the software in the product that is covered by this License, on a durable physical medium customarily used for software interchange, for a price no more than your reasonable cost of physically performing this conveying of source, or (2) access to copy the Corresponding Source from a network server at no charge.

- c) Convey individual copies of the object code with a copy of the written offer to provide the Corresponding Source. This alternative is allowed only occasionally and noncommercially, and only if you received the object code with such an offer, in accord with subsection 6b.
- d) Convey the object code by offering access from a designated place (gratis or for a charge), and offer equivalent access to the Corresponding Source in the same way through the same place at no further charge. You need not require recipients to copy the Corresponding Source along with the object code. If the place to copy the object code is a network server, the Corresponding Source may be on a different server (operated by you or a third party) that supports equivalent copying facilities, provided you maintain clear directions next to the object code saying where to find the Corresponding Source. Regardless of what server hosts the Corresponding Source, you remain obligated to ensure that it is available for as long as needed to satisfy these requirements.
- e) Convey the object code using peer-to-peer transmission, provided you inform other peers where the object code and Corresponding Source of the work are being offered to the general public at no charge under subsection 6d.

A separable portion of the object code, whose source code is excluded from the Corresponding Source as a System Library, need not be included in conveying the object code work.

A “User Product” is either (1) a “consumer product”, which means any tangible personal property which is normally used for personal, family, or household purposes, or (2) anything designed or sold for incorporation into a dwelling. In determining whether a product is a consumer product, doubtful cases shall be resolved in favor of coverage. For a particular product received by a particular user, “normally used” refers to a typical or common use of that class of product, regardless of the status of the particular user or of the way in which the particular user actually uses, or expects or is expected to use, the product. A product is a consumer product regardless of whether the product has substantial commercial, industrial or non-consumer uses, unless such uses represent the only significant mode of use of the product.

“Installation Information” for a User Product means any methods, procedures, authorization keys, or other information required to install and execute modified versions of a covered work in that User Product from a modified version of its Corresponding Source. The information must suffice to ensure that the continued functioning of the modified object code is in no case prevented or interfered with solely because modification has been made.

If you convey an object code work under this section in, or with, or specifically for use in, a User Product, and the conveying occurs as part of a transaction in which the right of possession and use of the User Product is transferred to the recipient in perpetuity or for a fixed term (regardless of how the transaction is characterized), the Corresponding Source conveyed under this section must be accompanied by the Installation Information. But this requirement does not apply if neither you nor any third party retains the ability to install modified object code on the User Product (for example, the work has been installed in ROM).

The requirement to provide Installation Information does not include a requirement to continue to provide support service, warranty, or updates for a work that has been modified or installed by the recipient, or for the User Product in which it has been modified or installed. Access to a network may be denied when the modification itself materially and adversely affects the operation of the network or violates the rules and protocols for communication across the network.

Corresponding Source conveyed, and Installation Information provided, in accord with this section must be in a format that is publicly documented (and with an implementation available to the public in source code form), and must require no special password or key for unpacking, reading or copying.

7. Additional Terms.

“Additional permissions” are terms that supplement the terms of this License by making exceptions from one or more of its conditions. Additional permissions that are applicable to the entire Program shall be treated as though they were included in this License, to the extent that they are valid under applicable law. If additional permissions apply only to part of the Program, that part may be used separately under those permissions, but the entire Program remains governed by this License without regard to the additional permissions.

When you convey a copy of a covered work, you may at your option remove any additional permissions from that copy, or from any part of it. (Additional permissions may be written to require their own removal in certain cases when you modify the work.) You may place additional permissions on material, added by you to a covered work, for which you have or can give appropriate copyright permission.

Notwithstanding any other provision of this License, for material you add to a covered work, you may (if authorized by the copyright holders of that material) supplement the terms of this License with terms:

- a) Disclaiming warranty or limiting liability differently from the terms of sections 15 and 16 of this License; or
- b) Requiring preservation of specified reasonable legal notices or author attributions in that material or in the Appropriate Legal Notices displayed by works containing it; or
- c) Prohibiting misrepresentation of the origin of that material, or requiring that modified versions of such material be marked in reasonable ways as different from the original version; or
- d) Limiting the use for publicity purposes of names of licensors or authors of the material; or
- e) Declining to grant rights under trademark law for use of some trade names, trademarks, or service marks; or
- f) Requiring indemnification of licensors and authors of that material by anyone who conveys the material (or modified versions of it) with contractual assumptions of liability to the recipient, for any liability that these contractual assumptions directly impose on those licensors and authors.

All other non-permissive additional terms are considered “further restrictions” within the meaning of section 10. If the Program as you received it, or any part of it, contains a notice stating that it is governed by this License along with a term that is a further restriction, you may remove that term. If a license document contains a further restriction but permits relicensing or conveying under this License, you may add to a covered work material governed by the terms of that license document, provided that the further restriction does not survive such relicensing or conveying.

If you add terms to a covered work in accord with this section, you must place, in the relevant source files, a statement of the additional terms that apply to those files, or a notice indicating where to find the applicable terms.

Additional terms, permissive or non-permissive, may be stated in the form of a separately written license, or stated as exceptions; the above requirements apply either way.

8. Termination.

You may not propagate or modify a covered work except as expressly provided under this License. Any attempt otherwise to propagate or modify it is void, and will automatically terminate your rights under this License (including any patent licenses granted under the third paragraph of section 11).

However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright holder, and you cure the violation prior to 30 days after your receipt of the notice.

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, you do not qualify to receive new licenses for the same material under section 10.

9. Acceptance Not Required for Having Copies.

You are not required to accept this License in order to receive or run a copy of the Program. Ancillary propagation of a covered work occurring solely as a consequence of using peer-to-peer transmission to receive a copy likewise does not require acceptance. However, nothing other than this License grants you permission to propagate or modify any covered work. These actions infringe copyright if you do not accept this License. Therefore, by modifying or propagating a covered work, you indicate your acceptance of this License to do so.

10. Automatic Licensing of Downstream Recipients.

Each time you convey a covered work, the recipient automatically receives a license from the original licensors, to run, modify and propagate that work, subject to this License. You are not responsible for enforcing compliance by third parties with this License.

An “entity transaction” is a transaction transferring control of an organization, or substantially all assets of one, or subdividing an organization, or merging organizations. If propagation of a covered work results from an entity transaction, each party to that transaction who receives a copy of the work also receives whatever licenses to the work the party's predecessor in interest had or could give under the previous paragraph, plus a right to possession of the Corresponding Source of the work from the predecessor in interest, if the predecessor has it or can get it with reasonable efforts.

You may not impose any further restrictions on the exercise of the rights granted or affirmed under this License. For example, you may not impose a license fee, royalty, or other charge for exercise of rights granted under this License, and you may not initiate litigation (including a cross-claim or counterclaim in a lawsuit) alleging that any patent claim is infringed by making, using, selling, offering for sale, or importing the Program or any portion of it.

11. Patents.

A “contributor” is a copyright holder who authorizes use under this License of the Program or a work on which the Program is based. The work thus licensed is called the contributor's “contributor version”.

A contributor's “essential patent claims” are all patent claims owned or controlled by the contributor, whether already acquired or hereafter acquired, that would be infringed by some manner, permitted by this License, of making, using, or selling its contributor version, but do not include claims that would be infringed only as a consequence of further modification of the contributor version. For purposes of this definition, “control” includes the right to grant patent sublicenses in a manner consistent with the requirements of this License.

Each contributor grants you a non-exclusive, worldwide, royalty-free patent license under the contributor's essential patent claims, to make, use, sell, offer for sale, import and otherwise run, modify and propagate the contents of its contributor version.

In the following three paragraphs, a “patent license” is any express agreement or commitment, however denominated, not to enforce a patent (such as an express permission to practice a patent or covenant not to sue for patent infringement). To “grant” such a patent license to a party means to make such an agreement or commitment not to enforce a patent against the party.

If you convey a covered work, knowingly relying on a patent license, and the Corresponding Source of the work is not available for anyone to copy, free of charge and under the terms of this License, through a publicly available network server or other

readily accessible means, then you must either (1) cause the Corresponding Source to be so available, or (2) arrange to deprive yourself of the benefit of the patent license for this particular work, or (3) arrange, in a manner consistent with the requirements of this License, to extend the patent license to downstream recipients. “Knowingly relying” means you have actual knowledge that, but for the patent license, your conveying the covered work in a country, or your recipient's use of the covered work in a country, would infringe one or more identifiable patents in that country that you have reason to believe are valid.

If, pursuant to or in connection with a single transaction or arrangement, you convey, or propagate by procuring conveyance of, a covered work, and grant a patent license to some of the parties receiving the covered work authorizing them to use, propagate, modify or convey a specific copy of the covered work, then the patent license you grant is automatically extended to all recipients of the covered work and works based on it.

A patent license is “discriminatory” if it does not include within the scope of its coverage, prohibits the exercise of, or is conditioned on the non-exercise of one or more of the rights that are specifically granted under this License. You may not convey a covered work if you are a party to an arrangement with a third party that is in the business of distributing software, under which you make payment to the third party based on the extent of your activity of conveying the work, and under which the third party grants, to any of the parties who would receive the covered work from you, a discriminatory patent license (a) in connection with copies of the covered work conveyed by you (or copies made from those copies), or (b) primarily for and in connection with specific products or compilations that contain the covered work, unless you entered into that arrangement, or that patent license was granted, prior to 28 March 2007.

Nothing in this License shall be construed as excluding or limiting any implied license or other defenses to infringement that may otherwise be available to you under applicable patent law.

12. No Surrender of Others' Freedom.

If conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot convey a covered work so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not convey it at all. For example, if you agree to terms that obligate you to collect a royalty for further conveying from those to whom you convey the Program, the only way you could satisfy both those terms and this License would be to refrain entirely from conveying the Program.

13. Use with the GNU Affero General Public License.

Notwithstanding any other provision of this License, you have permission to link or combine any covered work with a work licensed under version 3 of the GNU Affero General Public License into a single combined work, and to convey the resulting work. The terms of this License will continue to apply to the part which is the covered work,

but the special requirements of the GNU Affero General Public License, section 13, concerning interaction through a network will apply to the combination as such.

14. Revised Versions of this License.

The Free Software Foundation may publish revised and/or new versions of the GNU General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies that a certain numbered version of the GNU General Public License “or any later version” applies to it, you have the option of following the terms and conditions either of that numbered version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of the GNU General Public License, you may choose any version ever published by the Free Software Foundation.

If the Program specifies that a proxy can decide which future versions of the GNU General Public License can be used, that proxy's public statement of acceptance of a version permanently authorizes you to choose that version for the Program.

Later license versions may give you additional or different permissions. However, no additional obligations are imposed on any author or copyright holder as a result of your choosing to follow a later version.

15. Disclaimer of Warranty.

THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. Limitation of Liability.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MODIFIES AND/OR CONVEYS THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR

OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

17. Interpretation of Sections 15 and 16.

If the disclaimer of warranty and limitation of liability provided above cannot be given local legal effect according to their terms, reviewing courts shall apply local law that most closely approximates an absolute waiver of all civil liability in connection with the Program, unless a warranty or assumption of liability accompanies a copy of the Program in return for a fee.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively state the exclusion of warranty; and each file should have at least the “copyright” line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.>

Copyright (C) <year> <name of author>

This program is free software: you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation, either version 3 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program. If not, see <<http://www.gnu.org/licenses/>>.

Also add information on how to contact you by electronic and paper mail.

If the program does terminal interaction, make it output a short notice like this when it starts in an interactive mode:

<program> Copyright (C) <year> <name of author>

This program comes with ABSOLUTELY NO WARRANTY; for details type `show w'.

This is free software, and you are welcome to redistribute it

under certain conditions; type ``show c'` for details.

The hypothetical commands ``show w'` and ``show c'` should show the appropriate parts of the General Public License. Of course, your program's commands might be different; for a GUI interface, you would use an “about box”.

You should also get your employer (if you work as a programmer) or school, if any, to sign a “copyright disclaimer” for the program, if necessary. For more information on this, and how to apply and follow the GNU GPL, see <http://www.gnu.org/licenses/>.

The GNU General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Lesser General Public License instead of this License. But first, please read <http://www.gnu.org/philosophy/why-not-lgpl.html>.

Canvi de contrasenya en els diferents serveis.

Un cop implantat el sistema, tots els usuaris podran realitzar el canvi de contrasenya en els diferents serveis on han estat donats d'alta.

Per a realitzar aquest canvi de contrasenya cal definir una serie de conceptes per tal de quedí clar quines seràn les conseqüències d'efectuar un canvi de contrasenya.

El nostre sistema implantat disposa de dues bases de dades on hi figuren les dades de connexió dels usuaris. Una base de dades és la que està associada a les plataformes web IntraWeb i Moodle, i l'altra base de dades, és la que hem creat mitjançant un servidor LDAP.

En un principi (un cop fetes les migracions de dades corresponents) les dades de connexió coincideixen en les dues bases de dades, però no serà així si un usuari decideix canviar alguna contrasenya. Cal tenir aquest fet molt clar, ja que un usuari es pot pensar que si canvia la contrasenya de la IntraWeb i Moodle també ho farà del portal captiu (xarxa wi-fi) i del procés de validació contra el domini (quan volem entrar en un ordinador amb Windows XP) i no és el cas.

El següent esquema resol els dubtes i fa una aclaració de com varien les dades de connexió depenent d'on efectuem el canvi.

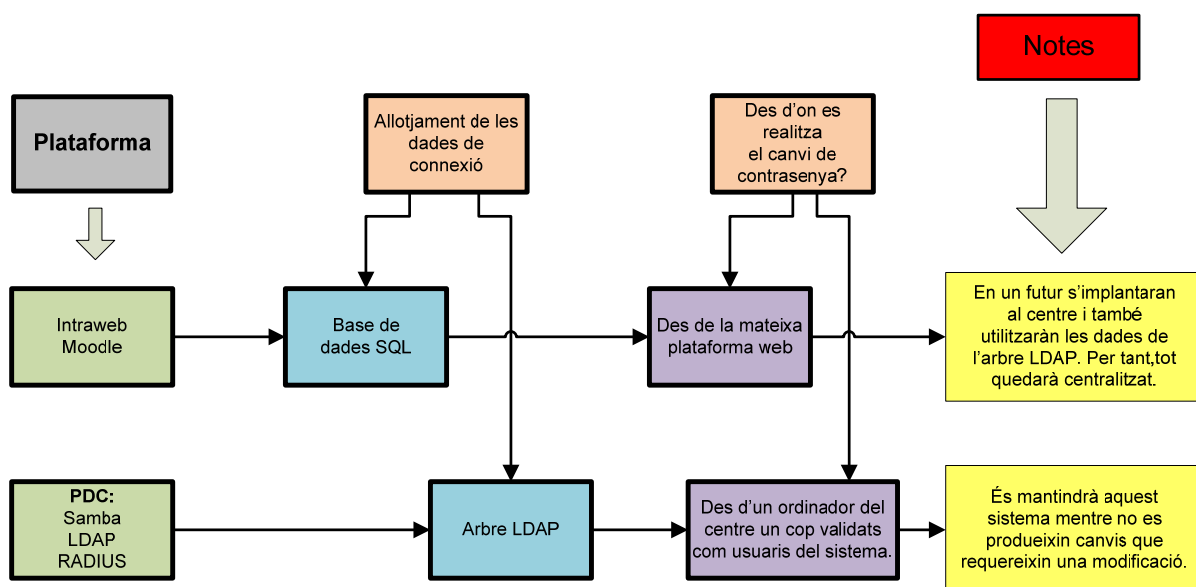


Figura 69: Canvis de contrasenya

Webgrafia

En aquest apartat es donen a conèixer els enllaços web que he utilitzat per a elaborar aquest treball de fi de carrera. Alguns d'ells parlen de configuració dels serveis i d'altres donen a conèixer el perquè de la seva utilització.

- <http://jroliva.wordpress.com/samba-ldap-debian-40-etch/>
- <http://cit3.idl.swin.edu.au/~533473X/index.php/HowTo:OpenLDAP+FreeRADIUS>
- [samba_como_pdcopenldap.pdf \(application/pdf Objeto\)](#)
http://rolandpish.files.wordpress.com/2007/10/samba_como_pdcopenldap.pdf
- [Blog de un administrador de sistemas: NSS y LDAP](#)
<http://www.logadmin.net/2006/03/nss-y-ldap.html>
- [XTEC. Nivell de configuracions dels centres – Projecte Heura](#)
http://www.xtec.cat/at_usuari/guies/heura/configuracio_centres/
- [Radius authentication using LDAP](#)
<http://tldp.org/HOWTO/archived/LDAP-Implementation-HOWTO/radius.html>
- [Webmin and Quota Configuration in Debian](#)
<http://www.debianhelp.co.uk/Webmin.htm>
- [nss ldap](#)
http://www.padl.com/OSS/nss_ldap.html
- [RADIUS - Wikipedia, la enciclopedia libre](#)
<http://es.wikipedia.org/wiki/RADIUS>
- [Apache-SSL](#)
http://www.apache-ssl.org/#What_is_Apache-SSL
- [Itinerancia - Wikipedia, la enciclopedia libre](#)
<http://es.wikipedia.org/wiki/Roaming>
- [Smbldap-Tools - Wikipedia, the free encyclopedia](#)
<http://en.wikipedia.org/wiki/Smbldap-Tools>
- [Live CD - Wikipedia, la enciclopedia libre](#)
http://es.wikipedia.org/wiki/CD_aut%C3%B3nomo

- [DebianLive - Debian Wiki](http://wiki.debian.org/DebianLive/)
<http://wiki.debian.org/DebianLive/>
- [LDAP - Wikipedia, la enciclopedia libre](http://es.wikipedia.org/wiki/LDAP)
<http://es.wikipedia.org/wiki/LDAP>
- [Samba \(programa\) - Wikipedia, la enciclopedia libre](http://es.wikipedia.org/wiki/Samba_(programa))
[http://es.wikipedia.org/wiki/Samba_\(programa\)](http://es.wikipedia.org/wiki/Samba_(programa))
- [phpLDAPadmin: LDAP browser to manager your LDAP server](http://phpldapadmin.sourceforge.net/)
<http://phpldapadmin.sourceforge.net/>
- [Servidor HTTP Apache - Wikipedia, la enciclopedia libre](http://es.wikipedia.org/wiki/Apache_http_server)
http://es.wikipedia.org/wiki/Apache_http_server
- [Secure Shell - Wikipedia, la enciclopedia libre](http://es.wikipedia.org/wiki/Secure_Shell)
http://es.wikipedia.org/wiki/Secure_Shell
- [OpenLDAP - wiki.GACQ.com](http://wiki.gacq.com/index.php/OpenLDAP#nscd)
<http://wiki.gacq.com/index.php/OpenLDAP#nscd>
- [Linux Servers](http://www.skullbox.net/linux.php)
<http://www.skullbox.net/linux.php>
- [WinSCP :: Introducció](http://winscp.net/eng/docs/lang:es)
<http://winscp.net/eng/docs/lang:es>
- [Csvtoldap.pl - Kolab wiki](http://wiki.kolab.org/index.php/Csvtoldap.pl)
<http://wiki.kolab.org/index.php/Csvtoldap.pl>
- <http://antonolsen.com/2007/05/01/export-thunderbird-contacts-and-import-into-gmail/>
- <http://www.openldap.org/faq/data/cache/347.html>
- <http://www.ibiblio.org/pub/micro/pc-stuff/Linux/docs/LuCaS/Tutoriales/doc-openldap-samba-cups-python/htmls/make-deleteHomedirectory.html>

Glossari

- [1] http://es.wikipedia.org/wiki/Controlador_de_dominio
- [2] http://es.wikipedia.org/wiki/Portal_cautivo
- [3] <http://www.freebsd.org/es/>
- [4] <http://www.fon.com/es>
- [5] http://es.wikipedia.org/wiki/Licencia_p%C3%BAblica_general_de_GNU
- [6] <http://www.xfce.org/?lang=en>
- [7] <http://ca.wikipedia.org/wiki/ISP>
- [8] <http://es.wikipedia.org/wiki/PAP>
- [9] <http://es.wikipedia.org/wiki/CHAP>.
- [10] http://es.wikipedia.org/wiki/Extensible_Authentication_Protocol
- [11] <http://es.wikipedia.org/wiki/L2TP>.
- [12] <http://es.wikipedia.org/wiki/Sftp>
- [13] <http://www.kde.org/>
- [14] <http://ca.wikipedia.org/wiki/RAID>
- [15] http://ca.wikipedia.org/wiki/Xarxa_de_llarg_abast
- [16] http://es.wikipedia.org/wiki/Red_de_%C3%A1rea_local
- [17] http://ca.wikipedia.org/wiki/Sistema_encastat
- [18] http://es.wikipedia.org/wiki/Bloque_de_arranque
- [19] http://ca.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol
- [20] <http://ca.wikipedia.org/wiki/HTTPS>.
- [21] http://es.wikipedia.org/wiki/Direcci%C3%B3n_MAC
- [22] http://ca.wikipedia.org/wiki/Extensible_Markup_Language
- [23] http://en.wikipedia.org/wiki/Comma-separated_values

- [24] <http://www.debian.org>
- [25] http://www.phpmyadmin.net/home_page/index.php
- [26] http://es.wikipedia.org/wiki/Algoritmo_MD5
- [27] http://en.wikipedia.org/wiki/Live_CD
- [28] [http://es.wikipedia.org/wiki/Cron_\(unix\)](http://es.wikipedia.org/wiki/Cron_(unix))

